

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/017758

International filing date: 30 November 2004 (30.11.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2003-410784
Filing date: 09 December 2003 (09.12.2003)

Date of receipt at the International Bureau: 27 January 2005 (27.01.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

02.12.2004

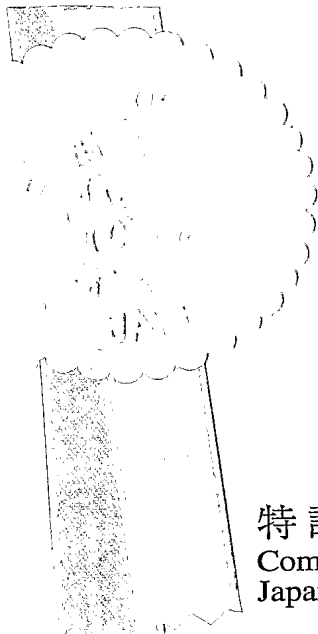
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 2 月 9 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 4 1 0 7 8 4
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 4 1 0 7 8 4]

出 願 人 松 下 電 器 産 業 株 式 有 限 公 司
Applicant(s):

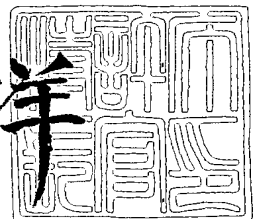


特許庁長官
Commissioner,
Japan Patent Office

2 0 0 5 年 1 月 1 4 日

小 川

洋



【書類名】 特許願
【整理番号】 2022550343
【提出日】 平成15年12月 9日
【あて先】 特許庁長官 殿
【国際特許分類】 G09L 1/00
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 野仲 真佐男
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 館林 誠
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 大森 基司
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100090446
 【弁理士】
 【氏名又は名称】 中島 司朗
【手数料の表示】
 【予納台帳番号】 014823
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9003742

【書類名】 特許請求の範囲**【請求項 1】**

可搬型の認証記録媒体と、前記認証記録媒体の正当性を認証する認証装置とからなる認証システムであって、

前記認証装置は、

前記認証記録媒体の正当性を検証するための認証情報を記憶している認証情報記憶手段と、

チャレンジデータを生成し、生成したチャレンジデータを記憶するデータ生成手段と、

前記チャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力手段と、

レスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取手段と、

前記認証情報を用いて、受け取ったレスポンスデータに第 1 変換を施して認証データを生成し、生成した認証データと前記チャレンジデータとが一致するか否かを検証する検証手段と、

前記検証手段にて、一致すると検証した場合に、前記認証記録媒体が正当であると決定する決定手段とを備え、

前記認証記録媒体は、

耐タンパ性を有し、自己の正当性を証明するための証明情報を記憶している証明情報記憶手段と、

前記認証装置より前記チャレンジデータを受け取るチャレンジデータ受取手段と、

前記証明情報を用いて、前記チャレンジデータに第 2 変換を施してレスポンスデータを生成するレスポンスデータ生成手段と、

生成したレスポンスデータを前記認証装置へ出力するレスポンスデータ出力手段とを備え、

前記第 1 変換は前記第 2 変換の逆変換である

ことを特徴とする認証システム。

【請求項 2】

可搬型の認証記録媒体の正当性を認証する認証装置であって、

前記認証記録媒体の正当性を検証するための認証情報を記憶している認証情報記憶手段と、

チャレンジデータを生成し、生成したチャレンジデータを記憶するデータ生成手段と、

前記チャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力手段と、

前記チャレンジデータより生成されたレスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取手段と、

受け取ったレスポンスデータと前記チャレンジデータと前記認証情報とを用いて、前記認証記録媒体の正当性を検証する検証手段と、

前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する決定手段と

を備えることを特徴とする認証装置。

【請求項 3】

前記認証記録媒体は、宅配業者が有し、

前記認証装置は、前記宅配業者による訪問を受ける者が有し、

前記認証記録媒体は、宅配業者による訪問を示す第 1 訪問情報を記憶しており、

前記認証装置は、さらに、

宅配業者による訪問を示す第 2 訪問情報を記憶している訪問情報記憶手段と、

第 1 訪問情報を前記認証記録媒体より受け取り、受け取った第 1 訪問情報と前記第 2 訪問情報とが一致するか否かの判断を行う判断手段とを備え、

前記決定手段は、前記判断手段にて受け取った第 1 訪問情報と前記第 2 訪問情報とが一致すると判断した場合、及び前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する

ことを特徴とする請求項 2 に記載の認証装置。

【請求項 4】

前記認証記録媒体は、暗号鍵を記憶しており、
前記認証情報は、前記暗号化鍵に対応する復号鍵であり、
前記レスポンスデータ受取手段は、前記暗号化鍵を用いて前記チャレンジデータを暗号化したレスポンスデータを受け取り、
前記検証手段は、前記レスポンスデータを、前記復号鍵を用いて復号して認証データを生成し、生成した認証データと前記データ生成手段にて記憶している前記チャレンジデータとが一致するか否かを検証する
ことを特徴とする請求項 3 に記載の認証装置。

【請求項 5】

前記暗号化鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報であり、
前記認証装置は、さらに、
所有者証明情報に対応する、前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報を受け付ける受付手段を備え、
前記認証情報記憶手段は、受け付けた所有者認証情報を記憶し、
前記レスポンスデータ受取手段は、前記所有者証明情報を用いて前記チャレンジデータを暗号化したレスポンスデータを受け取り、
前記検証手段は、前記レスポンスデータを、前記所有者認証情報を用いて復号して認証データを生成する
ことを特徴とする請求項 4 に記載の認証装置。

【請求項 6】

前記認証情報は、秘密鍵であり、
前記認証記録媒体は、前記秘密鍵と同一の秘密鍵を記憶しており、
前記レスポンスデータ受取手段は、秘密鍵暗号により前記チャレンジデータを暗号化したレスポンスデータを前記認証記録媒体より受け取り、
前記検証手段は、前記チャレンジデータを、前記秘密鍵を用いた秘密鍵暗号により暗号化して暗号化認証データを生成し、生成した暗号化認証データと、受け取ったレスポンスデータとが一致するか否かを検証する
ことを特徴とする請求項 3 に記載の認証装置。

【請求項 7】

前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報であり、
前記認証装置は、さらに、
所有者認証情報を受け付ける受付手段を備え、
前記認証情報記憶手段は、受け付けた所有者認証情報を記憶し、
前記検証手段は、前記チャレンジデータを、前記所有者認証情報を用いて暗号化して暗号化認証データを生成する
ことを特徴とする請求項 6 に記載の認証装置。

【請求項 8】

前記認証記録媒体は、秘密鍵を記憶しており、
前記認証情報は、前記秘密鍵に対応する公開鍵であり、
前記レスポンスデータ受取手段は、前記秘密鍵を用いて前記チャレンジデータの電子署名であるレスポンスデータを受け取り、
前記検証手段は、受け取ったレスポンスデータと前記公開鍵と前記チャレンジデータとを用いて署名検証する
ことを特徴とする請求項 3 に記載の認証装置。

【請求項 9】

前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応しており、

前記認証装置は、さらに、
所有者証明情報に対応する、前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報を受け付ける受付手段を備え、
前記認証情報記憶手段は、前記認証情報を記憶する代わりに、受け付けた所有者認証情報を記憶し、
前記検証手段は、前記所有者認証情報から前記秘密鍵に対応する公開鍵を生成し、生成した公開鍵と前記チャレンジデータと前記レスポンスデータとを用いて署名検証することを特徴とする請求項 8 に記載の認証装置。

【請求項 10】

前記認証装置は、さらに、
宅配業者による訪問の正当性を検証するための訪問検証情報を記憶している検証情報記憶手段と、
訪問検証チャレンジデータを生成し、生成した訪問検証チャレンジデータを記憶する訪問検証データ生成手段と、
前記訪問検証チャレンジデータを前記認証記録媒体へ出力する訪問検証チャレンジデータ出力手段と、
前記訪問検証チャレンジデータより生成された訪問検証レスポンスデータを前記認証記録媒体より受け取る訪問検証レスポンスデータ受取手段と、
受け取った訪問検証レスポンスデータと、前記訪問検証情報と前記訪問検証チャレンジデータとを用いて、宅配業者による訪問の正当性を検証する訪問検証手段とを備え、
前記決定手段は、前記判断手段にて受け取った第 1 訪問情報と前記第 2 訪問情報とが一致すると判断した場合、前記訪問検証手段にて肯定的に検証した場合、及び前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定することを特徴とする請求項 3 に記載の認証装置。

【請求項 11】

前記認証装置は、さらに、
認証情報を配信する配信装置とネットワークを介して接続されており、
前記認証装置は、さらに、
前記配信装置より配信される認証情報を受信する受信手段と、
前記認証情報を前記認証情報記憶手段に書き込む書込手段と
を備えることを特徴とする請求項 3 に記載の認証装置。

【請求項 12】

前記チャレンジデータ出力手段は、前記チャレンジデータを出力する代わりに、前記チャレンジデータから変換チャレンジ情報を生成し、生成した変換チャレンジ情報を前記認証記録媒体へ出力することを特徴とする請求項 3 に記載の認証装置。

【請求項 13】

前記変換チャレンジ情報は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる情報である
ことを特徴とする請求項 12 に記載の認証装置。

【請求項 14】

前記レスポンスデータ受取手段は、前記レスポンスデータを受け取る代わりに、前記レスポンスデータより生成された変換レスポンス情報を受け取り、受け取った変換レスポンス情報より前記レスポンスデータを生成することを特徴とする請求項 3 に記載の認証装置。

【請求項 15】

前記変換レスポンス情報は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる情報である
ことを特徴とする請求項 14 に記載の認証装置。

【請求項 16】

前記認証装置は、さらに、
自己を識別する装置識別子を記憶している識別子記憶手段と、
前記決定手段にて、前記認証記録媒体が正当であると決定した場合に、前記装置識別子を前記認証記録媒体へ出力する識別子出力手段とを
備えることを特徴とする請求項 3 に記載の認証装置。

【請求項 17】

前記認証装置は、携帯電話機である
ことを特徴とする請求項 2 乃至 16 に記載の認証装置。

【請求項 18】

可搬型の認証記録媒体の正当性を認証する認証装置であって、
チャレンジデータを生成するための認証情報を記憶している認証情報記憶手段と、
第 1 データを生成し、生成した第 1 データを記憶するデータ生成手段と、
前記認証情報を用いて、前記第 1 データを変換して、チャレンジデータを生成する変換手段と、
生成したチャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力手段と
、
前記チャレンジデータより生成されたレスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取手段と、
受け取ったレスポンスデータと前記第 1 データとが一致するか否かを検証する検証手段と、
前記検証手段にて、一致すると検証した場合に、前記認証記録媒体が正当であると決定する決定手段と
を備えることを特徴とする認証装置。

【請求項 19】

前記認証記録媒体は、宅配業者にて所有され、
前記認証装置は、前記宅配業者による訪問を受ける者が有し、
前記認証記録媒体は、前記宅配業者による訪問を示す第 1 訪問情報を記憶しており、
前記認証装置は、さらに、
前記宅配業者による訪問を示す第 2 訪問情報を記憶している訪問情報記憶手段と、
第 1 訪問情報を前記認証記録媒体より受け取り、受け取った第 1 訪問情報と前記第 2 訪問情報とが一致するか否かの判断を行う判断手段とを備え、
前記決定手段は、前記判断手段にて受け取った第 1 訪問情報と前記第 2 訪問情報とが一致すると判断した場合、及び前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する
ことを特徴とする請求項 18 に記載の認証装置。

【請求項 20】

前記認証記録媒体は、秘密鍵を記憶しており、
前記認証情報は、前記秘密鍵に対応する公開鍵であり、
前記変換手段は、前記公開鍵を用いて、前記第 1 データを暗号化してチャレンジデータを生成し、
前記レスポンスデータ受取手段は、前記秘密鍵を用いて前記チャレンジデータを復号したレスポンスデータを受け取る
ことを特徴とする請求項 19 に記載の認証装置。

【請求項 21】

前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応しており、
前記認証装置は、さらに、
所有者証明情報に対応する、前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報を受け付ける受付手段を備え、
前記認証情報記憶手段は、前記認証情報を記憶する代わりに、受け付けた所有者認証情

報を記憶し、

前記変換手段は、記憶している所有者認証情報を用いて前記暗号化鍵に対応する公開鍵を生成し、生成した公開鍵を用いて前記第 1 データを暗号化してチャレンジデータを生成する

ことを特徴とする請求項 20 に記載の認証装置。

【請求項 22】

認証装置により認証がなされる可搬型の認証記録媒体であって、

耐タンパ性を有し、自己の正当性を証明するための証明情報を記憶している証明情報記憶手段と、

前記認証装置よりチャレンジデータを受け取るチャレンジデータ受取手段と、

前記証明情報を用いて前記チャレンジデータからレスポンスデータを生成するレスポンスデータ生成手段と、

生成したレスポンスデータを前記認証装置へ出力するレスポンスデータ出力手段と

を備えることを特徴とする認証記録媒体。

【請求項 23】

前記認証記録媒体は、宅配業者が有し、

前記認証記録媒体は、さらに、

宅配業者による訪問を示す訪問情報を記憶している訪問情報記憶手段と、

前記訪問情報を前記認証装置へ出力する訪問情報出力手段と

を備えることを特徴とする請求項 22 に記載の認証記録媒体。

【請求項 24】

前記証明情報は、暗号化鍵であり、

前記レスポンスデータ生成手段は、前記暗号化鍵を用いて前記チャレンジデータを暗号化して、レスポンスデータを生成する

ことを特徴とする請求項 23 に記載の認証記録媒体。

【請求項 25】

前記暗号化鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報であり、

前記レスポンスデータ生成手段は、前記所有者証明情報を用いて、前記チャレンジデータを暗号化して、レスポンスデータを生成する

ことを特徴とする請求項 24 に記載の認証記録媒体。

【請求項 26】

前記認証情報は、秘密鍵であり、

前記チャレンジデータは、前記秘密鍵に対応する公開鍵を用いて、前記認証装置により生成されたデータが暗号化されたデータであり、

前記レスポンスデータ生成手段は、前記秘密鍵を用いて受け取ったチャレンジデータを復号して、レスポンスデータを生成する

ことを特徴とする請求項 23 に記載の認証記録媒体。

【請求項 27】

前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応した鍵であり、

前記公開鍵は、前記所有者証明情報に対応する前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報を用いて前記認証記録媒体にて生成された鍵である

ことを特徴とする請求項 26 に記載の認証記録媒体。

【請求項 28】

前記認証情報は、秘密鍵であり、

前記レスポンスデータ生成手段は、前記秘密鍵を用いて受け取ったチャレンジデータの電子署名であるレスポンスデータを生成する

ことを特徴とする請求項 23 に記載の認証記録媒体。

【請求項 29】

前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応した鍵である

ことを特徴とする請求項 28 に記載の認証記録媒体。

【請求項 30】

前記チャレンジデータ受取手段は、前記チャレンジデータを受け取る代わりに、前記チャレンジデータから生成された変換チャレンジ情報を受け取り、受け取った変換チャレンジ情報より前記チャレンジデータを生成する

ことを特徴とする請求項 23 に記載の認証記録媒体。

【請求項 31】

前記変換チャレンジ情報は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる情報である

ことを特徴とする請求項 30 に記載の認証記録媒体。

【請求項 32】

前記レスポンスデータ出力手段は、前記レスポンスデータを出力する代わりに、前記レスポンスデータから変換レスポンス情報を生成し、生成した変換レスポンス情報を出力する

ことを特徴とする請求項 23 に記載の認証記録媒体。

【請求項 33】

前記変換レスポンス情報は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる情報である

ことを特徴とする請求項 32 に記載の認証記録媒体。

【請求項 34】

前記認証記録媒体は、さらに、

前記認証装置より、前記認証装置を識別する装置識別子を受け取る識別子受取手段と、受け取った装置識別子を記憶する識別子記憶手段とを

備えることを特徴とする請求項 23 に記載の認証記録媒体。

【請求項 35】

可搬型の認証記録媒体の正当性を認証する認証装置に用いられる認証方法であって、

前記認証装置は、

前記認証記録媒体の正当性を検証するための認証情報を記憶している認証情報記憶手段を備え、

前記認証方法は、

チャレンジデータを生成し、生成したチャレンジデータを記憶するデータ生成ステップと、

前記チャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力ステップと

、前記チャレンジデータより生成されたレスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取ステップと、

受け取ったレスポンスデータと前記チャレンジデータと前記認証情報とを用いて、前記認証記録媒体の正当性を検証する検証ステップと、

前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する決定ステップと

を含むことを特徴とする認証方法。

【請求項 36】

可搬型の認証記録媒体の正当性を認証する認証装置に用いられる認証プログラムであって、

前記認証装置は、

前記認証記録媒体の正当性を検証するための認証情報を記憶している認証情報記憶手段を備え、

前記認証プログラムは、

チャレンジデータを生成し、生成したチャレンジデータを記憶するデータ生成ステップと、
前記チャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力ステップと、
前記チャレンジデータより生成されたレスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取ステップと、
受け取ったレスポンスデータと前記チャレンジデータと前記認証情報とを用いて、前記認証記録媒体の正当性を検証する検証ステップと、
前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する決定ステップと
を含むことを特徴とする認証プログラム。

【請求項 37】

可搬型の認証記録媒体の正当性を認証する認証装置に用いられる認証プログラムを記録しているコンピュータ読み取り可能な認証プログラム記録媒体であって、
前記認証装置は、
前記認証記録媒体の正当性を検証するための認証情報を記憶している認証情報記憶手段を備え、
前記認証プログラムは、
チャレンジデータを生成し、生成したチャレンジデータを記憶するデータ生成ステップと、
前記チャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力ステップと、
前記チャレンジデータより生成されたレスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取ステップと、
受け取ったレスポンスデータと前記チャレンジデータと前記認証情報とを用いて、前記認証記録媒体の正当性を検証する検証ステップと、
前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する決定ステップと
を含むことを特徴とする認証プログラム記録媒体。

【請求項 38】

認証装置により認証がなされる可搬型の認証記録媒体に用いられる証明方法であって、
前記認証記録媒体は、
耐タンパ性を有し、自己の正当性を証明するための証明情報を記憶している証明情報記憶手段を備え、
前記証明方法は、
前記認証装置よりチャレンジデータを受け取るチャレンジデータ受取ステップと、
前記証明情報を用いて前記チャレンジデータからレスポンスデータを生成するレスポンスデータ生成ステップと、
生成したレスポンスデータを前記認証装置へ出力するレスポンスデータ出力ステップと
を含むことを特徴とする証明方法。

【請求項 39】

認証装置により認証がなされる可搬型の認証記録媒体に用いられる証明プログラムであって、
前記認証記録媒体は、
耐タンパ性を有し、自己の正当性を証明するための証明情報を記憶している証明情報記憶手段を備え、
前記証明プログラムは、
前記認証装置よりチャレンジデータを受け取るチャレンジデータ受取ステップと、
前記証明情報を用いて前記チャレンジデータからレスポンスデータを生成するレスポンスデータ生成ステップと、

生成したレスポンスデータを前記認証装置へ出力するレスポンスデータ出力ステップとを含むことを特徴とする証明プログラム。

【請求項 4 0】

認証装置により認証がなされる可搬型の認証記録媒体に用いられる証明プログラムを記録しているコンピュータ読み取り可能な証明プログラム記録媒体であって、

前記認証記録媒体は、

耐タンパ性を有し、自己の正当性を証明するための証明情報を記憶している証明情報記憶手段を備え、

前記証明プログラムは、

前記認証装置よりチャレンジデータを受け取るチャレンジデータ受取ステップと、

前記証明情報を用いて前記チャレンジデータからレスポンスデータを生成するレスポンスデータ生成ステップと、

生成したレスポンスデータを前記認証装置へ出力するレスポンスデータ出力ステップとを含むことを特徴とする証明プログラム記録媒体。

【書類名】明細書

【発明の名称】認証システム

【技術分野】

【0001】

本発明は、記録媒体の所有者の身元を認証する技術に関する。

【背景技術】

【0002】

従来、宅内にいる者が、訪問者の身元をインターホンやテレビドアホンなどを利用して確認する方法が一般的に用いられている。

しかしながら、上記の方法では、訪問者が容姿や声を偽ることによって、宅内にいる者を欺くことができるため、宅内にいる者が、訪問者の身元を確実に確認することは困難である。

【0003】

そこで、特許文献1に示すような個人情報表示システムが開示されている。この個人情報表示システムは、個人情報及び個人特定情報を予め記憶しているサーバと、個人特定情報を通信回線を介してサーバに送信するユーザ端末とを有し、サーバは、予め記憶している個人特定情報とユーザ端末から送信された個人特定情報とを照合し、照合結果に応じて、個人特定情報と関連付けられて記憶している個人情報をユーザ端末に送信し、ユーザ端末は、サーバから受信した個人情報を表示する。この個人情報表示システムによって、宅配業者等の訪問者の身分を確実に確認することが可能になる。

【特許文献1】特開2003-108529号公報

【発明の開示】

【発明が解決しようとする課題】

【0004】

しかしながら、上記に示す個人情報表示システムに限らず様々な形態にて訪問者の確認を行うシステムの要望がある。

そこで、本発明は、従来技術とは異なる、訪問者の身元の認証を行うことのできる認証システム、認証装置、認証記録媒体、認証方法、認証プログラム、認証プログラム記録媒体、証明方法、証明プログラム及び証明プログラム記録媒体を提供することを目的とする。

【課題を解決するための手段】

【0005】

上記目的を達成するために、本発明は、可搬型の認証記録媒体と、前記認証記録媒体の正当性を認証する認証装置とからなる認証システムであって、前記認証装置は、前記認証記録媒体の正当性を検証するための認証情報を記憶している認証情報記憶手段と、チャレンジデータを生成し、生成したチャレンジデータを記憶するデータ生成手段と、前記チャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力手段と、レスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取手段と、前記認証情報を用いて、受け取ったレスポンスデータに第1変換を施して認証データを生成し、生成した認証データと前記チャレンジデータとが一致するか否かを検証する検証手段と、前記検証手段にて、一致すると検証した場合に、前記認証記録媒体が正当であると決定する決定手段とを備え、前記認証記録媒体は、耐タンパ性を有し、自己の正当性を証明するための証明情報を記憶している証明情報記憶手段と、前記認証装置より前記チャレンジデータを受け取るチャレンジデータ受取手段と、前記証明情報を用いて、前記チャレンジデータに第2変換を施してレスポンスデータを生成するレスポンスデータ生成手段と、生成したレスポンスデータを前記認証装置へ出力するレスポンスデータ出力手段とを備え、前記第1変換は前記第2変換の逆変換であることを特徴とする。

【発明の効果】

【0006】

課題を解決するための手段に示した構成によると、認証システムは、認証記録媒体の正

当性を検証する場合に、レスポンスデータを受け取った認証装置にて行う。このとき、レスポンスデータを生成する際に用いる証明情報は、耐タンパ性を有する証明情報記憶手段にて記憶されているため、第三者にて改竄されることはない。そのため、認証記録媒体が正当であると決定された場合には、認証記録媒体の所有者を正当な所有者であると決定することができる。

【0007】

また、本発明は、可搬型の認証記録媒体の正当性を認証する認証装置であって、前記認証記録媒体の正当性を検証するための認証情報を記憶している認証情報記憶手段と、チャレンジデータを生成し、生成したチャレンジデータを記憶するデータ生成手段と、前記チャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力手段と、前記チャレンジデータより生成されたレスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取手段と、受け取ったレスポンスデータと前記チャレンジデータと前記認証情報とを用いて、前記認証記録媒体の正当性を検証する検証手段と、前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定する決定手段とを備えることを特徴とする。

【0008】

この構成によると、認証装置は、当該認証装置にて記憶しているチャレンジデータと認証情報と認証記録媒体より受け取ったレスポンスデータとを用いて、認証記録媒体の正当性を検証する。これにより、認証記録媒体が正当であると決定された場合には、認証記録媒体の所有者を正当な所有者であると決定することができる。

ここで、前記認証記録媒体は、宅配業者が有し、前記認証装置は、前記宅配業者による訪問を受ける者が有し、前記認証記録媒体は、宅配業者による訪問を示す第1訪問情報を記憶しており、前記認証装置は、さらに、宅配業者による訪問を示す第2訪問情報を記憶している訪問情報記憶手段と、第1訪問情報を前記認証記録媒体より受け取り、受け取った第1訪問情報と前記第2訪問情報とが一致するか否かの判断を行う判断手段とを備え、前記決定手段は、前記判断手段にて受け取った第1訪問情報と前記第2訪問情報とが一致すると判断した場合、及び前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定するとしてもよい。

【0009】

この構成によると、認証装置は、さらに、第1訪問情報と第2訪問情報とが一致するか否かを判断を行い、認証記録媒体が正当であることを決定するための条件が、さらに付加されていることにより、認証記録媒体の正当性がより確かなものとなる。つまり、認証記録媒体の所有者の正当性がより確かなものとなるため、宅配業者による訪問が確かな訪問であると決定することができる。

【0010】

ここで、前記認証記録媒体は、暗号鍵を記憶しており、前記認証情報は、前記暗号化鍵に対応する復号鍵であり、前記レスポンスデータ受取手段は、前記暗号化鍵を用いて前記チャレンジデータを暗号化したレスポンスデータを受け取り、前記検証手段は、前記レスポンスデータを、前記復号鍵を用いて復号して認証データを生成し、生成した認証データと前記データ生成手段にて記憶している前記チャレンジデータとが一致するか否かを検証するとしてもよい。

【0011】

この構成によると、認証装置は、チャレンジデータが認証記録媒体が記憶している暗号鍵にて暗号化されたレスポンスデータを、前記暗号鍵に対応する復号鍵を用いて、復号して、認証データを生成し、生成した認証データとチャレンジデータとが一致するか否かを検証することができる。つまり、認証装置は、暗号処理を利用して、認証記録媒体の認証を行うことができる。

【0012】

ここで、前記暗号化鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報であり、前記認証装置は、さらに、所有者証明情報に対応する、前記認証記録媒体

の所有者の生体科学的特徴を示す所有者認証情報を受け付ける受付手段を備え、前記認証情報記憶手段は、受け付けた所有者認証情報を記憶し、前記レスポンスデータ受取手段は、前記所有者証明情報を用いて前記チャレンジデータを暗号化したレスポンスデータを受け取り、前記検証手段は、前記レスポンスデータを、前記所有者認証情報を用いて復号して認証データを生成するとしてもよい。

【0013】

この構成によると、認証装置は、認証記録媒体の所有者の生体科学的特徴を示す情報を用いて、レスポンスデータを復号して認証データを生成することができる。

ここで、前記認証情報は、秘密鍵であり、前記認証記録媒体は、前記秘密鍵と同一の秘密鍵を記憶しており、前記レスポンスデータ受取手段は、秘密鍵暗号により前記チャレンジデータを暗号化したレスポンスデータを前記認証記録媒体より受け取り、前記検証手段は、前記チャレンジデータを、前記秘密鍵を用いた秘密鍵暗号により暗号化して暗号化認証データを生成し、生成した暗号化認証データと、受け取ったレスポンスデータとが一致するか否かを検証するとしてもよい。

【0014】

この構成によると、認証装置は、チャレンジデータが認証記録媒体にて記憶している秘密鍵を用いた秘密鍵暗号により暗号化されたレスポンスデータと、チャレンジデータが当該認証装置が記憶している前記秘密鍵と同一の秘密鍵を用いた秘密鍵暗号により暗号化された暗号化認証データとを用いて、認証記録媒体の正当性を検証することができる。

ここで、前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報であり、前記認証装置は、さらに、所有者認証情報を受け付ける受付手段を備え、前記認証情報記憶手段は、受け付けた所有者認証情報を記憶し、前記検証手段は、前記チャレンジデータを、前記所有者認証情報を用いて暗号化して暗号化認証データを生成するとしてもよい。

【0015】

この構成によると、認証装置は、認証記録媒体の所有者の生体科学的特徴を示す情報を用いて、チャレンジデータを暗号化して暗号化認証データを生成することができる。

ここで、前記認証記録媒体は、秘密鍵を記憶しており、前記認証情報は、前記秘密鍵に対応する公開鍵であり、前記レスポンスデータ受取手段は、前記秘密鍵を用いて前記チャレンジデータの電子署名であるレスポンスデータを受け取り、前記検証手段は、受け取ったレスポンスデータと前記公開鍵と前記チャレンジデータとを用いて署名検証するとしてもよい。

【0016】

この構成によると、認証装置は、チャレンジデータの電子署名であるレスポンスデータを受け取り、チャレンジデータと、公開鍵と、受け取ったレスポンスデータとを用いて署名検証を行うことにより、認証記録媒体の正当性を検証することができる。

ここで、前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応しており、前記認証装置は、さらに、

所有者証明情報に対応する、前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報を受け付ける受付手段を備え、前記認証情報記憶手段は、前記認証情報を記憶する代わりに、受け付けた所有者認証情報を記憶し、前記検証手段は、前記所有者認証情報から前記秘密鍵に対応する公開鍵を生成し、生成した公開鍵と前記チャレンジデータと前記レスポンスデータとを用いて署名検証するとしてもよい。

【0017】

この構成によると、認証装置は、認証記録媒体の所有者の生体科学的特徴を示す情報と、チャレンジデータと、レスポンスデータとを用いて、署名検証することができる。

ここで、前記認証装置は、さらに、宅配業者による訪問の正当性を検証するための訪問検証情報を記憶している検証情報記憶手段と、訪問検証チャレンジデータを生成し、生成した訪問検証チャレンジデータを記憶する訪問検証データ生成手段と、前記訪問検証チャレンジデータを前記認証記録媒体へ出力する訪問検証チャレンジデータ出力手段と、前記

訪問検証チャレンジデータより生成された訪問検証レスポンスデータを前記認証記録媒体より受け取る訪問検証レスポンスデータ受取手段と、受け取った訪問検証レスポンスデータと、前記訪問検証情報と前記訪問検証チャレンジデータとを用いて、宅配業者による訪問の正当性を検証する訪問検証手段とを備え、前記決定手段は、前記判断手段にて受け取った第1訪問情報と前記第2訪問情報とが一致すると判断した場合、前記訪問検証手段にて肯定的に検証した場合、及び前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定するとしてもよい。

【0018】

この構成によると、宅配業者による訪問の正当性の検証を行い、認証記録媒体が正当であることを決定するための条件が、さらに付加されていることにより、認証記録媒体の正当性がより確かなものとなる。つまり、宅配業者による訪問がより確かな訪問であると決定することができる。

ここで、前記認証装置は、さらに、認証情報を配信する配信装置とネットワークを介して接続されており、前記認証装置は、さらに、前記配信装置より配信される認証情報を受信する受信手段と、前記認証情報を前記認証情報記憶手段に書き込む書込手段とを備えるとしてもよい。

【0019】

この構成によると、認証装置は、配信装置より認証情報を受信し、受信した認証情報を認証情報記憶手段へ書き込むことができる。これにより、宅配業者は、訪問する前に、事前に配信装置を用いて、訪問時の認証に必要な認証情報を配信することができ、認証装置は、宅配業者による訪問を受けた際に行う認証に必要な認証情報のみを、事前に受信することができる。

【0020】

ここで、前記チャレンジデータ出力手段は、前記チャレンジデータを出力する代わりに、前記チャレンジデータから変換チャレンジ情報を生成し、生成した変換チャレンジ情報を前記認証記録媒体へ出力するとしてもよい。

この構成によると、認証装置は、チャレンジデータの代わりに、チャレンジデータより生成した変換チャレンジ情報を認証記録媒体へ出力することができる。

【0021】

ここで、前記変換チャレンジ情報は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる情報であるとしてもよい。

この構成によると、認証装置は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる変換チャレンジ情報を、認証記録媒体へ出力することができる。

【0022】

ここで、前記レスポンスデータ受取手段は、前記レスポンスデータを受け取る代わりに、前記レスポンスデータより生成された変換レスポンス情報を受け取り、受け取った変換レスポンス情報より前記レスポンスデータを生成するとしてもよい。

この構成によると、認証装置は、レスポンスデータの代わりに、レスポンスデータより生成された変換レスポンス情報を認証記録媒体より受け取り、受け取った変換レスポンス情報よりレスポンスデータを生成することができる。

【0023】

ここで、前記変換レスポンス情報は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる情報であるとしてもよい。

この構成によると、認証装置は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる変換レスポンス情報を、認証記録媒体より受け取り、受け取った変換レスポンス情報よりレスポンスデータを生成することができる。

【0024】

ここで、前記認証装置は、さらに、自己を識別する装置識別子を記憶している識別子記憶手段と、前記決定手段にて、前記認証記録媒体が正当であると決定した場合に、前記装

置識別子を前記認証記録媒体へ出力する識別子出力手段とを備えるとしてもよい。

この構成によると、認証装置は、認証記録媒体が正当であると決定した場合に、装置識別子を認証記録媒体へ出力することができる。

【0025】

また、本発明は、可搬型の認証記録媒体の正当性を認証する認証装置であって、チャレンジデータを生成するための認証情報を記憶している認証情報記憶手段と、第1データを生成し、生成した第1データを記憶するデータ生成手段と、前記認証情報を用いて、前記第1データを変換して、チャレンジデータを生成する変換手段と、生成したチャレンジデータを前記認証記録媒体へ出力するチャレンジデータ出力手段と、前記チャレンジデータより生成されたレスポンスデータを前記認証記録媒体より受け取るレスポンスデータ受取手段と、受け取ったレスポンスデータと前記第1データとが一致するか否かを検証する検証手段と、前記検証手段にて、一致すると検証した場合に、前記認証記録媒体が正当であると決定する決定手段とを備えることを特徴とする。

【0026】

この構成によると、認証装置は、当該認証装置にて記憶している第1データと認証情報と認証記録媒体より受け取ったレスポンスデータとを用いて、認証記録媒体の正当性を検証する。これにより、認証記録媒体が正当であると決定された場合には、認証記録媒体の所有者を正当な所有者であると決定することができる。

ここで、前記認証記録媒体は、宅配業者にて所有され、前記認証装置は、前記宅配業者による訪問を受ける者が有し、前記認証記録媒体は、前記宅配業者による訪問を示す第1訪問情報を記憶しており、前記認証装置は、さらに、前記宅配業者による訪問を示す第2訪問情報を記憶している訪問情報記憶手段と、第1訪問情報を前記認証記録媒体より受け取り、受け取った第1訪問情報と前記第2訪問情報とが一致するか否かの判断を行う判断手段とを備え、前記決定手段は、前記判断手段にて受け取った第1訪問情報と前記第2訪問情報とが一致すると判断した場合、及び前記検証手段にて肯定的に検証した場合に、前記認証記録媒体が正当であると決定するとしてもよい。

【0027】

この構成によると、認証装置は、さらに、第1訪問情報と第2訪問情報とが一致するか否かを判断を行い、認証記録媒体が正当であることを決定するための条件が、さらに付加されていることにより、認証記録媒体の正当性がより確かなものとなる。つまり、認証記録媒体の所有者の正当性がより確かなものとなるため、宅配業者による訪問が確かな訪問であると決定することができる。

【0028】

ここで、前記認証記録媒体は、秘密鍵を記憶しており、前記認証情報は、前記秘密鍵に対応する公開鍵であり、前記変換手段は、前記公開鍵を用いて、前記第1データを暗号化してチャレンジデータを生成し、前記レスポンスデータ受取手段は、前記秘密鍵を用いて前記チャレンジデータを復号したレスポンスデータを受け取るとしてもよい。

この構成によると、認証装置は、公開鍵暗号を用いて、認証記録媒体の正当性を検証することができる。

【0029】

ここで、前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応しており、前記認証装置は、さらに、所有者証明情報に対応する、前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報を受け付ける受付手段を備え、前記認証情報記憶手段は、前記認証情報を記憶する代わりに、受け付けた所有者認証情報を記憶し、前記変換手段は、記憶している所有者認証情報を用いて前記暗号化鍵に対応する公開鍵を生成し、生成した公開鍵を用いて前記第1データを暗号化してチャレンジデータを生成するとしてもよい。

【0030】

この構成によると、認証装置は、認証記録媒体の所有者の生体科学的特徴を示す情報に対応する公開鍵を生成し、生成した公開鍵を用いて、チャレンジデータを生成することが

できる。

また、本発明は、認証装置により認証がなされる可搬型の認証記録媒体であって、耐タンパ性を有し、自己の正当性を証明するための証明情報を記憶している証明情報記憶手段と、前記認証装置よりチャレンジデータを受け取るチャレンジデータ受取手段と、前記証明情報を用いて前記チャレンジデータからレスポンスデータを生成するレスポンスデータ生成手段と、生成したレスポンスデータを前記認証装置へ出力するレスポンスデータ出力手段とを備えることを特徴とする。

【0031】

この構成によると、認証記録媒体は、証明情報を用いて、認証装置より受け取ったチャレンジデータからレスポンスデータを生成し、生成したレスポンスデータを認証装置へ出力することができる。このとき、レスポンスデータを生成する際に用いる証明情報は、耐タンパ性を有する証明情報記憶手段にて記憶されているため、第三者にて改竄されることはない。これにより、認証記録媒体は、証明情報を用いて生成したレスポンスデータを自己の正当性を証明するデータとすることができる。また、自己の正当性を証明するために認証情報そのものを認証装置へ出力する代わりに、レスポンスデータを認証装置へ出力しているため、認証記録媒体と認証装置との間におけるデータ盗聴に対するセキュリティが向上される。

【0032】

ここで、前記認証記録媒体は、宅配業者が有し、前記認証記録媒体は、さらに、宅配業者による訪問を示す訪問情報を記憶している訪問情報記憶手段と、前記訪問情報を前記認証装置へ出力する訪問情報出力手段とを備えるとしてもよい。

この構成によると、認証記録媒体は、さらに、訪問情報を認証装置へ出力することができる。

【0033】

ここで、前記証明情報は、暗号化鍵であり、前記レスポンスデータ生成手段は、前記暗号化鍵を用いて前記チャレンジデータを暗号して、レスポンスデータを生成するとしてもよい。

この構成によると、認証記録媒体は、暗号鍵を用いて、チャレンジデータを暗号化したレスポンスデータを生成することができる。

【0034】

ここで、前記暗号化鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報であり、前記レスポンスデータ生成手段は、前記所有者証明情報を用いて、前記チャレンジデータを暗号化して、レスポンスデータを生成するとしてもよい。

この構成によると、暗号鍵を認証記録媒体の所有者の生体科学的特徴を示す情報として、レスポンスデータを生成することができる。

【0035】

ここで、前記認証情報は、秘密鍵であり、前記チャレンジデータは、前記秘密鍵に対応する公開鍵を用いて、前記認証装置により生成されたデータが暗号化されたデータであり、前記レスポンスデータ生成手段は、前記秘密鍵を用いて受け取ったチャレンジデータを復号して、レスポンスデータを生成するとしてもよい。

この構成によると、認証記録媒体は、秘密鍵を用いて、認証装置より受け取ったチャレンジデータを復号して、レスポンスデータを生成することができる。つまり、公開鍵暗号を利用して、レスポンスデータを生成することができる。

【0036】

ここで、前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応した鍵であり、前記公開鍵は、前記所有者証明情報に対応する前記認証記録媒体の所有者の生体科学的特徴を示す所有者認証情報を用いて前記認証記録媒体にて生成された鍵であるとしてもよい。

この構成によると、認証記録媒体は、当該認証記録媒体の所有者の生体科学的特徴を示す情報に対応する秘密鍵を用いて、レスポンスデータを生成することができる。

【0037】

ここで、前記認証情報は、秘密鍵であり、前記レスポンスデータ生成手段は、前記秘密鍵を用いて受け取ったチャレンジデータの電子署名であるレスポンスデータを生成するとしてもよい。

この構成によると、認証記録媒体は、レスポンスデータとして、チャレンジデータの電子署名を生成することができる。

【0038】

ここで、前記秘密鍵は、前記認証記録媒体の所有者の生体科学的特徴を示す所有者証明情報に対応した鍵であるとしてもよい。

この構成によると、認証記録媒体は、当該認証記録媒体の所有者の生体科学的特徴を示す情報に対応する秘密鍵を用いて、チャレンジデータの電子署名を生成することができる。

【0039】

ここで、前記チャレンジデータ受取手段は、前記チャレンジデータを受け取る代わりに、前記チャレンジデータから生成された変換チャレンジ情報を受け取り、受け取った変換チャレンジ情報より前記チャレンジデータを生成するとしてもよい。

この構成によると、認証記録媒体は、チャレンジデータの代わりに、チャレンジデータより生成された変換チャレンジ情報を認証装置より受け取り、受け取った変換チャレンジ情報よりチャレンジデータを生成することができる。

【0040】

ここで、前記変換チャレンジ情報は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる情報であるとしてもよい。

この構成によると、認証記録媒体は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる変換チャレンジ情報を、認証装置より受け取り、受け取った変換チャレンジ情報よりチャレンジデータを生成することができる。

【0041】

ここで、前記レスポンスデータ出力手段は、前記レスポンスデータを出力する代わりに、前記レスポンスデータから変換レスポンス情報を生成し、生成した変換レスポンス情報を出力するとしてもよい。

この構成によると、認証記録媒体は、レスポンスデータの代わりに、レスポンスデータより生成した変換レスポンス情報を認証装置へ出力することができる。

【0042】

ここで、前記変換レスポンス情報は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる情報であるとしてもよい。

この構成によると、認証記録媒体は、光信号、バーコード、QRコード、赤外線信号、及び音声信号のうち何れかからなる変換レスポンス情報を、認証装置へ出力することができる。

【0043】

ここで、前記認証記録媒体は、さらに、前記認証装置より、前記認証装置を識別する装置識別子を受け取る識別子受取手段と、受け取った装置識別子を記憶する識別子記憶手段とを備えるとしてもよい。

この構成によると、認証記録媒体は、認証装置より装置識別子を受け取り、記憶することができる。

【発明を実施するための最良の形態】**【0044】****1. 第1の実施の形態**

本発明に係る第1の実施の形態としての身元認証システム1について説明する。

1.1 身元認証システム1の概要

身元認証システム1は、図1に示すように、認証カード10、11、・・・、12とユーザ端末20とカードリーダー30とから構成されている。

【0045】

認証カード10、11、・・・、12は、それぞれ利用者宅へ訪問する異なる訪問業者（例えば、宅配便の業者）が所有するカードである。認証カード10には、認証カード10自身の正当性を証明するための訪問業者固有の身元証明鍵を予め記憶している。つまり、認証カード11、・・・、12には、認証カード10に記憶されている身元証明鍵とは異なる身元証明鍵がそれぞれ予め記憶されていることになる。身元証明鍵は、訪問業者にて安全に管理されている。なお、ここでは、身元認証システム1の概要についての説明を認証カード10とユーザ端末20とカードリーダー30とを用いて行う。

【0046】

ユーザ端末20及びカードリーダー30は、訪問業者から配布された装置であり、ユーザ端末20には、認証カード10の正当性を検証するための身元認証鍵が予め記憶されている。

ユーザ端末20は、利用者の宅内に配置されており、カードリーダー30は、利用者の宅外（例えば、玄関先）に配置されており、ユーザ端末20とカードリーダー30とは、ケーブル40にて接続されている。

【0047】

身元認証システム1は、認証カード10がカードリーダー30に挿入されると、認証カード10に記憶している身元証明鍵と、ユーザ端末20に記憶している身元認証鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行い、認証結果をユーザ端末20の表示部203にて表示する。

なお、ここで用いる暗号処理は、秘密鍵による暗号処理である。秘密鍵による暗号処理の一例は、DESである。DESについては、公知であるので説明を省略するが、身元証明鍵と身元認証鍵とが同一の鍵となることは、言うまでもない。

【0048】

また、身元認証システム1において、認証カード11、・・・、12のうち何れかの認証カードがカードリーダー30に挿入された場合も同様の動作を行うため、説明は省略する。

1. 2 認証カード10の構成

ここでは、認証カード10の構成について説明する。認証カード10は、ICを内蔵している可搬型の記録媒体であり、一例として、ICカード機能付メモリカードである。認証カード10は、図2に示すように、証明鍵記憶部101、制御部102及び入出力部103から構成されている。

【0049】

認証カード10は、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード10は、その機能を達成する。

なお、認証カード11、・・・、12は、認証カード10と同様の構成を有しているため、説明は省略する。

【0050】**(1) 証明鍵記憶部101**

証明鍵記憶部101は、耐タンパ性を有しており、身元証明鍵と、身元証明鍵を識別する証明鍵IDとからなる組を1つ記憶している。上述したように、ここで記憶されている身元証明鍵は、認証カード10自身の正当性を証明するための訪問業者固有の鍵であり、訪問業者にて安全に管理されている。

【0051】

以降の説明において、必要に応じて、身元証明鍵として「SK1」を用いて説明する。

(2) 制御部102

制御部102は、カードリーダー30より入出力部103を介して、証明鍵IDを要求する旨のID要求情報を受け取ると、証明鍵記憶部101より証明鍵IDを取得し、取得し

た証明鍵 ID を入出力部 103 を介してカードリーダー 30 へ出力する。

【0052】

さらに、制御部 102 は、カードリーダー 30 より乱数「N」を受け取ると、証明鍵記憶部 101 より身元証明鍵「SK1」を取得し、取得した身元証明鍵「SK1」を用いて、カードリーダー 30 より受け取った乱数「N」に対して暗号化を施し、暗号化情報 Enc (SK1、N) を生成する。制御部 102 は、生成した暗号化情報を入出力部 103 を介してカードリーダー 30 へ出力する。ここで、Enc (SK1、N) は、乱数「N」が身元証明鍵「SK1」にて暗号化された情報であることを意味する。

【0053】

(3) 入出力部 103

入出力部 103 は、カードリーダー 30 より受け取った情報を制御部 102 へ出力し、制御部 102 から受け取った情報をカードリーダー 30 へ出力する。

1. 3 ユーザ端末 20 の構成

ここでは、ユーザ端末 20 の構成について説明する。ユーザ端末 20 は、カードリーダー 30 に挿入された認証カード 10 の認証を行う。ユーザ端末 20 は、図 3 に示すように、認証鍵記憶部 201、認証部 202、表示部 203 及び入出力部 204 から構成されている。

【0054】

ユーザ端末 20 は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記 ROM 又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末 20 は、その機能を達成する。

【0055】

(1) 認証鍵記憶部 201

認証鍵記憶部 201 は、耐タンパ性を有しており、図 4 に一例として示すように、鍵情報テーブル T100 を備えている。

鍵情報テーブル T100 は、身元認証鍵と認証鍵 ID とからなる組を複数記憶するための領域を備えている。

【0056】

身元認証鍵は、カードリーダー 30 の挿入された認証カードの正当性を検証するための鍵であり、上述したように身元証明鍵と同一のものである。

認証鍵 ID は、身元認証鍵を識別する識別子であり、証明鍵 ID と同一の識別子にて対応付けされている。これにより、身元認証鍵と身元証明鍵との対応付けが可能となる。

また、鍵情報テーブル T100 にて記憶されている身元認証鍵の個数は、訪問業者の数と同じ数である。

【0057】

つまり、認証カード 10、11、・・・、12 のそれぞれに記憶されている証明鍵 ID と身元証明鍵との組に対応する、認証鍵 ID と身元認証鍵とからなる組が記憶されている。

(2) 認証部 202

認証部 202 は、乱数を記憶する乱数記憶領域 250 及びカードリーダー 30 より入出力部 204 を介して受け取った証明鍵 ID を記憶する ID 記憶領域 251 を有している。

【0058】

認証部 202 は、カードリーダー 30 より入出力部 204 を介して、カードリーダー 30 に認証カード 10 が挿入されたことを検知した旨を示す検知情報と、証明鍵 ID とを受け取り、受け取った証明鍵 ID を ID 記憶領域 251 に記憶する。次に、認証部 202 は、乱数「N」を生成し、生成した乱数「N」を入出力部 204 を介してカードリーダー 30 へ出力し、生成した乱数「N」を乱数記憶領域 250 に記憶する。

【0059】

さらに、認証部 202 は、カードリーダー 30 より入出力部 204 を介して、暗号化情報 Enc (SK1、N) を受け取る。次に、ID 記憶領域 251 にて記憶している証明鍵 ID と一致する認証鍵 ID と対応する身元認証鍵を鍵情報テーブル T100 より取得し、取得した身元認証鍵を用いて、暗号化情報 Enc (SK1、N) の復号を行い、復号により得られた復号結果と、乱数記憶領域 250 にて記憶している乱数「N」とが一致するか否かを判断する。

【0060】

復号結果と乱数「N」とが一致する場合には、認証部 202 は、カードリーダー 30 に挿入された認証カードが正当な認証カードであると認証し、認証結果として訪問者が正当な訪問者である旨を示す正当訪問者情報を生成し、生成した正当訪問者情報を表示部 203 へ出力する。復号結果と乱数「N」とが一致しない場合には、認証部 202 は、カードリーダー 30 に挿入された認証カードが不正な認証カードであると認証し、認証結果として訪問者が不正な訪問者である旨を示す不正訪問者情報を生成し、生成した不正訪問者情報を表示部 203 へ出力する。さらに、認証部 202 は、乱数記憶領域 250 に記憶している乱数「N」の消去、及び ID 記憶領域 251 に記憶している証明鍵 ID の消去を行う。

【0061】

(3) 表示部 203

表示部 203 は、例えば、ディスプレイを備え、認証部 202 より受け取った認証結果の情報を外部に対して表示する。

(4) 入出力部 204

入出力部 204 は、カードリーダー 30 より受け取った情報を認証部 202 へ出力し、認証部 202 から受け取った情報をカードリーダー 30 へ出力する。

【0062】

1. 4 カードリーダー 30

カードリーダー 30 は、図 3 に示すように、カード読取部 301 及び入出力部 302 から構成されている。

カードリーダー 30 は、具体的には、マイクロプロセッサ、ROM、RAM などから構成されるコンピュータシステムである。前記 ROM には、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、カードリーダー 30 は、その機能を達成する。

【0063】

(1) カード読取部 301

カード読取部 301 は、認証カード 10 が挿入されたことの検知を行う。カード読取部 301 は、認証カード 10 が挿入されたことを検知すると、検知情報及び ID 要求情報を生成し、生成した ID 要求情報を認証カード 10 へ出力する。次に、認証カード 10 より証明鍵 ID を受け取ると、受け取った証明鍵 ID と、生成した検知情報とを入出力部 302 を介してユーザ端末 20 へ出力する。

【0064】

さらに、カード読取部 301 は、ユーザ端末 20 より入出力部 302 を介して、乱数「N」を受け取ると、受け取った乱数「N」を認証カード 10 へ出力する。カード読取部 301 は、認証カード 10 より暗号化情報 Enc (SK1、N) を受け取ると、受け取った暗号化情報 Enc (SK1、N) を入出力部 302 を介してユーザ端末 20 へ出力する。

(2) 入出力部 302

入出力部 302 は、ユーザ端末 20 より受け取った情報をカード読取部 301 へ出力し、カード読取部 301 から受け取った情報をユーザ端末 20 へ出力する。

【0065】

1. 5 身元認証処理の動作

ここでは、認証カード 10 がカードリーダー 30 に挿入されてからユーザ端末 20 にて認証を行うまでの処理である身元認証処理の動作について、図 5 に示す流れ図を用いて説明する。

カードリーダー30は、認証カード10が挿入されたことを検知すると（ステップS5）、検知情報及びID要求情報を生成し、生成したID要求情報を認証カード10へ出力する（ステップS10）。

【0066】

認証カード10は、カードリーダー30よりID要求情報を受け取ると、証明鍵記憶部101にて記憶している証明鍵IDを取得し、取得した証明鍵IDをカードリーダー30へ出力する（ステップS15）。

カードリーダー30は、認証カード10より証明鍵IDを受け取ると（ステップS20）、受け取った証明鍵IDと、ステップS10にて生成した検知情報とをユーザ端末20へ出力する（ステップS25）。

【0067】

ユーザ端末20は、カードリーダー30より証明鍵IDと検知情報とを受け取ると、受け取った証明鍵IDをID記憶領域251に記憶する（ステップS30）。次に、ユーザ端末20は、乱数「N」を生成し、生成した乱数「N」をカードリーダー30へ出力し、さらに、生成した乱数「N」を乱数記憶領域250に記憶する（ステップS35）。

カードリーダー30は、ユーザ端末20より乱数「N」を受け取ると、受け取った乱数「N」を認証カード10へ出力する（ステップS40）。

【0068】

認証カード10は、カードリーダー30より乱数「N」を受け取ると（ステップS45）、受け取った乱数「N」を証明鍵記憶部101にて記憶している身元証明鍵を用いて暗号化し、暗号化情報を生成し、生成した暗号化情報をカードリーダー30へ出力する（ステップS50）。

カードリーダー30は、認証カード10より暗号化情報を受け取ると、受け取った暗号化情報をユーザ端末20へ出力する（ステップS55）。

【0069】

ユーザ端末20は、カードリーダー30より暗号化情報を受け取ると、受け取った暗号化情報と認証鍵記憶部201にて記憶している身元認証鍵とを用いて、認証処理を行う（ステップS60）。

1.6 認証処理

ここでは、身元認証処理のステップS60にて行われる認証処理について、図6に示す流れ図を用いて説明する。

【0070】

ユーザ端末20は、認証カード10よりカードリーダー30を介して暗号化情報を受け取る（ステップS100）。次に、ユーザ端末20は、身元認証処理のステップS30にてID記憶領域251に記憶した証明鍵IDと一致する認証鍵IDと対応付けられた身元認証鍵を鍵情報テーブルT100より取得する（ステップS105）。さらに、ユーザ端末20は、取得した身元認証鍵を用いて、ステップS100にて受け取った暗号化情報を復号する（ステップS110）。

【0071】

次に、ユーザ端末20は、復号して得られた復号結果と、身元認証処理のステップS35にて乱数記憶領域250に記憶した乱数「N」とが一致するか否かの判断を行う（ステップS115）。

一致すると判断する場合には（ステップS115における「YES」）、正当訪問者情報を生成し、生成した正当訪問者情報を表示し（ステップS120）、乱数記憶領域250に記憶している乱数「N」、及びID記憶領域251に記憶している証明鍵IDをそれぞれ消去し（ステップS130）、処理を終了する。

【0072】

一致しないと判断する場合には（ステップS115における「NO」）、不正訪問者情報を生成し、生成した不正訪問者情報を表示し（ステップS125）、乱数記憶領域250に記憶している乱数「N」、及びID記憶領域251に記憶している証明鍵IDをそれ

ぞれ消去し（ステップ S130）、処理を終了する。

2. 第2の実施の形態

ここでは、本発明に係る第2の実施の形態としての身元認証システム1Aについて説明する。

【0073】

身元認証システム1では、身元認証鍵をユーザ端末20の認証鍵記憶部201に予め記憶したが、身元認証システム1Aでは、ユーザ端末が利用者に配布された後に、訪問業者より身元認証鍵を配布する。

2. 1 身元認証システム1Aの概要

身元認証システム1Aは、図7に示すように、認証カード10A、11A、・・・、12Aと、ユーザ端末20Aと、カードリーダー30Aと、配信装置50Aとから構成されている。カードリーダー30Aとユーザ端末20Aとは、ケーブル40Aにて接続されている。

【0074】

認証カード10A、11A、・・・、12Aは、訪問業者より利用者宅へ訪問する訪問者一人一人に割り当てられており、各認証カードには、それぞれ異なる身元証明鍵を予め記憶している。つまり、利用者宅へ訪問する訪問者と身元証明鍵とが対応付けられていることになる。

ここで、図7には、図示していないが、ユーザ端末20Aと同様の構成を有するユーザ端末21A、・・・、22Aも配信装置50Aとインターネットを介して接続されている。また、ユーザ端末21A、・・・、22Aはカードリーダー30Aと同様の構成を有するカードリーダー31A、・・・、32Aとそれぞれ接続されている。

【0075】

ここでは、認証カード10Aとユーザ端末20Aとカードリーダー30Aとを用いて、身元認証システム1Aの概要について説明する。なお、認証カード11A、・・・、12Aは、認証カード10Aと同様であり、ユーザ端末21A、・・・、22Aは、ユーザ端末20Aと同様であり、カードリーダー31A、・・・、32Aは、カードリーダー30Aと同様であるため、説明は省略する。

【0076】

身元認証システム1Aでは、訪問業者が利用者宅へ訪問する前に、訪問者に対応する身元認証鍵をユーザ端末20Aへインターネットを介して送信する。認証カード10Aがカードリーダー30Aに挿入されると、ユーザ端末20Aは、認証カード10Aに記憶されている身元証明鍵と、配信装置50Aより事前に受信して記憶している身元認証鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行い、認証結果を表示部203Aにて表示する。

【0077】

ここで用いる暗号処理は、身元認証システム1と同様に秘密鍵による暗号処理である。また、身元認証システム1と同様に身元証明鍵と身元認証鍵とが同一の鍵となることは、言うまでもない。

2. 2 配信装置50A

配信装置50Aは、訪問者が利用者宅へ訪問する前に、訪問者に対応する身元認証鍵をユーザ端末20Aへ送信する装置である。配信装置50Aは、図8に示すように、配信鍵記憶部501A、制御部502A、操作部503A及び送信部504Aから構成されている。

【0078】

配信装置50Aは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、モデムなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、配信装置50Aは、その機能を達成する。

【0079】

(1) 配信鍵記憶部 501A

配信鍵記憶部 501A は、図 9 に一例として示すように、配信鍵情報テーブル T200 を備えている。

配信鍵情報テーブル T200 は、訪問者 ID と身元認証鍵とからなる組を複数記憶するための領域を備えている。

【0080】

訪問者 ID は、訪問者を識別する識別子であり、身元認証鍵は、身元証明鍵と同一の鍵であり、訪問者 ID と対応付けられている。

なお、ここで記憶されている身元認証鍵の個数は、訪問者の人数、つまり認証カードの個数と同一となる。

また、身元認証鍵と訪問者 ID とを対応付けることにより、訪問者 ID に対応する身元認証鍵を記憶している認証カードを訪問者に割り当てることができる。

【0081】

(2) 制御部 502A

制御部 502A は、操作部 503A より、身元認証鍵の登録を示す情報と、訪問者 ID と、身元認証鍵とを受け取ると、受け取った訪問者 ID と身元認証鍵とを対応付けて、配信鍵記憶部 501A へ書き込む。

制御部 502A は、操作部 503A より身元認証鍵をユーザ端末 20A へ配信する旨の情報と、訪問者 ID とからなる配信情報を受け取ると、受け取った配信情報に含まれる訪問者 ID と対応する身元認証鍵を配信鍵情報テーブル T200 より取得する。制御部 502A は、取得した身元認証鍵をユーザ端末 20A へ送信部 504A を介して送信する。

【0082】

(3) 操作部 503A

操作部 503A は、配信装置 50A の操作者の操作により、身元認証鍵の登録を示す情報と、訪問者 ID と、身元認証鍵とを受け付けると、受け付けた身元認証鍵の登録を示す情報と、訪問者 ID と、身元認証鍵とを制御部 502A へ出力する。

また、操作部 503A は、操作者の操作により、配信情報を受け付けると、受け付けた配信情報を制御部 502A へ出力する。

【0083】

なお、操作者は、利用者宅へ訪問する訪問者自身に限らず、訪問業者に属する者であればよい。

(4) 送信部 504A

送信部 504A は、制御部 502A より受け取った情報をユーザ端末 20A へインターネットを介して出力する。

【0084】

2. 3 認証カード 10A

ここでは、認証カード 10A の構成について説明する。認証カード 10A は、IC を内蔵している可搬型の記録媒体であり、一例として、IC カード機能付メモリカードである。認証カード 10A は、図 10 に示すように、証明鍵記憶部 101A、制御部 102A 及び入出力部 103A から構成されている。

【0085】

認証カード 10A は、具体的には、マイクロプロセッサ、ROM、RAM などから構成されるコンピュータシステムである。前記 ROM には、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード 10A は、その機能を達成する。

なお、認証カード 11A、・・・、12A は、認証カード 10A と同様の構成を有しているため、説明は省略する。

【0086】

(1) 証明鍵記憶部 101A

証明鍵記憶部 101A は、耐タンパ性を有しており、訪問者に対応する身元証明鍵を 1 つ記憶している。

以降の説明において、必要に応じて、身元証明鍵として「SK1」を用いて説明する。

(2) 制御部 102A

制御部 102A は、カードリーダー 30A より乱数「N」を受け取ると、証明鍵記憶部 101A より身元証明鍵「SK1」を取得し、取得した身元証明鍵「SK1」を用いて、カードリーダー 30A より受け取った乱数「N」に対して暗号化を施し、暗号化情報 Enc (SK1、N) を生成する。制御部 102A は、生成した暗号化情報を入出力部 103A を介してカードリーダー 30A へ出力する。

【0087】

(3) 入出力部 103A

入出力部 103A は、認証カード 10 の入出力部 103 と同様であるため、説明は省略する。

2. 4 ユーザ端末 20A の構成

ここでは、ユーザ端末 20A の構成について説明する。ユーザ端末 20A は、図 11 に示すように、認証鍵記憶部 201A、認証部 202A、表示部 203A、入出力部 204A 及び受信部 205A から構成されている。

【0088】

ユーザ端末 20A は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記 ROM 又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末 20A は、その機能を達成する。

【0089】

また、上記の身元認証システム 1A の概要にて示したように、ユーザ端末 21A、・・・、22A は、ユーザ端末 20A と同様の構成であるため、説明は省略する。

(1) 認証鍵記憶部 201A

認証鍵記憶部 201A は、耐タンパ性を有しており、配信装置 50A よりインターネットを介して受信した身元認証鍵を記憶する領域を有している。

【0090】

(2) 受信部 205A

受信部 205A は、配信装置 50A よりインターネットを介して、身元認証鍵を受信すると、受信した身元認証鍵を認証鍵記憶部 201A へ書き込む。

これにより、ユーザ端末 20A は、訪問者に対応する身元認証鍵を事前に記憶することができる。

【0091】

(3) 認証部 202A

認証部 202A は、乱数を記憶する乱数記憶領域 250A を有している。

認証部 202A は、カードリーダー 30A より入出力部 204A を介して、カードリーダー 30A に認証カード 10A が挿入されたことを検知した旨を示す検知情報を受け取ると、乱数「N」を生成し、生成した乱数「N」を入出力部 204A を介してカードリーダー 30A へ出力し、生成した乱数「N」を乱数記憶領域 250A に記憶する。

【0092】

さらに、認証部 202A は、カードリーダー 30A より入出力部 204A を介して、暗号化情報 Enc (SK1、N) を受け取ると、認証鍵記憶部 201A にて事前に記憶している身元認証鍵を認証鍵記憶部 201A より取得し、取得した身元認証鍵を用いて、暗号化情報 Enc (SK1、N) の復号を行い、復号により得られた復号結果と、乱数記憶領域 250A にて記憶している乱数「N」とが一致するか否かを判断する。

【0093】

復号結果と乱数「N」とが一致する場合には、認証部 202A は、カードリーダー 30A

に挿入された認証カードが正当な認証カードであると認証し、認証結果として訪問者が正当な訪問者である旨を示す正当訪問者情報を生成し、生成した正当訪問者情報を表示部 203A へ出力する。復号結果と乱数「N」とが一致しない場合には、認証部 202A は、カードリーダー 30A に挿入された認証カードが不正な認証カードであると認証し、認証結果として訪問者が不正な訪問者である旨を示す不正訪問者情報を生成し、生成した不正訪問者情報を表示部 203A へ出力する。さらに、認証部 202A は、認証鍵記憶部 201A にて記憶している身元認証鍵の消去及び乱数記憶領域 250A に記憶している乱数「N」の消去を行う。

【0094】

(4) 表示部 203A

表示部 203A は、ユーザ端末 20 の表示部 203 と同様であるため、説明は省略する。

(5) 入出力部 204A

入出力部 204A は、ユーザ端末 20 の入出力部 204 と同様であるため、説明は省略する。

【0095】

2. 5 カードリーダー 30A

カードリーダー 30A は、図 11 に示すように、カード読取部 301A 及び入出力部 302A から構成されている。

カードリーダー 30A は、具体的には、マイクロプロセッサ、ROM、RAM などから構成されるコンピュータシステムである。前記 ROM には、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、カードリーダー 30A は、その機能を達成する。

【0096】

なお、上記の身元認証システム 1A の概要にて示したように、カードリーダー 31A、
・ ・ ・、32A は、カードリーダー 30A と同様の構成であるため、説明は省略する。

(1) カード読取部 301A

カード読取部 301A は、認証カード 10A が挿入されたことの検知を行う。カード読取部 301A は、認証カード 10A が挿入されたことを検知すると、検知情報を生成し、生成した検知情報を入出力部 302A を介してユーザ端末 20A へ出力する。

【0097】

さらに、カード読取部 301A は、ユーザ端末 20A より入出力部 302A を介して、乱数「N」を受け取ると、受け取った乱数「N」を認証カード 10A へ出力する。カード読取部 301A は、認証カード 10A より暗号化情報 Enc (SK1, N) を受け取ると、受け取った暗号化情報 Enc (SK1, N) を入出力部 302A を介してユーザ端末 20A へ出力する。

【0098】

(2) 入出力部 302A

入出力部 302A は、カードリーダー 30 の入出力部 302 と同様であるため、説明は省略する。

2. 6 配信処理の動作

ここでは、身元認証鍵を事前に配信する配信処理について、図 12 に示す流れ図を用いて、説明する。

【0099】

配信装置 50A は、利用者の操作により配信情報を受け付けると (ステップ S200)、受け付けた配信情報に含まれる訪問者 ID に対応する身元認証鍵を配信鍵記憶部 501A より取得する (ステップ S205)。次に、配信装置 50A は、取得した身元認証鍵をユーザ端末 20A へインターネットを介して配信する (ステップ S210)。

ユーザ端末 20A は、配信装置 50A より身元認証鍵を受信すると (ステップ S215)、受信した身元認証鍵を認証鍵記憶部 201A へ書き込む (ステップ S220)。

【0100】**2. 7 身元認証処理の動作**

ここでは、認証カード10Aがカードリーダー30Aに挿入されてからユーザ端末20Aにて認証を行うまでの処理である身元認証処理の動作について、図13に示す流れ図を用いて説明する。

カードリーダー30Aは、認証カード10Aが挿入されたことを検知すると（ステップS250）、検知情報を生成し、生成した検知情報をユーザ端末20Aへ出力する（ステップS255）。

【0101】

ユーザ端末20Aは、カードリーダー30Aより検知情報を受け取ると、乱数「N」を生成し、生成した乱数「N」をカードリーダー30Aへ出力し、さらに、生成した乱数「N」を乱数記憶領域250Aに記憶する（ステップS260）。

カードリーダー30Aは、ユーザ端末20Aより乱数「N」を受け取ると、受け取った乱数「N」を認証カード10Aへ出力する（ステップS265）。

【0102】

認証カード10Aは、カードリーダー30Aより乱数「N」を受け取ると（ステップS270）、受け取った乱数「N」を証明鍵記憶部101Aにて記憶している身元証明鍵を用いて暗号化して、暗号化情報を生成し、生成した暗号化情報をカードリーダー30Aへ出力する（ステップS275）。

カードリーダー30Aは、認証カード10Aより暗号化情報を受け取ると、受け取った暗号化情報をユーザ端末20Aへ出力する（ステップS280）。

【0103】

ユーザ端末20Aは、カードリーダー30Aより暗号化情報を受け取ると、受け取った暗号化情報と認証鍵記憶部201Aにて記憶している身元認証鍵とを用いて、認証処理を行う（ステップS285）。

2. 8 認証処理

ここでは、身元認証処理のステップS285にて行われる認証処理について、図14に示す流れ図を用いて説明する。

【0104】

ユーザ端末20Aは、認証カード10Aよりカードリーダー30Aを介して暗号化情報を受け取る（ステップS300）。次に、ユーザ端末20Aは、配信装置50Aより事前に配信された身元認証鍵を認証鍵記憶部201Aより取得する（ステップS305）。さらに、ユーザ端末20Aは、取得した身元認証鍵を用いて、ステップS300にて受け取った暗号化情報を復号する（ステップS310）。

【0105】

次に、ユーザ端末20Aは、復号して得られた復号結果と、身元認証処理のステップS260にて乱数記憶領域250Aに記憶した乱数「N」とが一致するか否かの判断を行う（ステップS315）。

一致すると判断する場合には（ステップS315における「YES」）、正当訪問者情報を生成し、生成した正当訪問者情報を表示し（ステップS320）、認証鍵記憶部201Aにて記憶している身元認証鍵及び乱数記憶領域250Aに記憶している乱数「N」を消去し（ステップS330）、処理を終了する。

【0106】

一致しないと判断する場合には（ステップS315における「NO」）、不正訪問者情報を生成し、生成した不正訪問者情報を表示し（ステップS325）、認証鍵記憶部201Aにて記憶している身元認証鍵及び乱数記憶領域250Aに記憶している乱数「N」を消去し（ステップS330）、処理を終了する。

3. 第3の実施の形態

ここでは、本発明に係る第3の実施の形態としての身元認証システム1Bについて説明する。

【0107】

身元認証システム1Bでは、訪問者が利用者宅に訪問時に、身元認証鍵として訪問者の生体科学的特徴を示すバイオメトリックス情報を用いて、認証カードが正当な認証カードであるか否かの認証を行う。

3. 1 身元認証システム1Bの概要

身元認証システム1Bは、図15に示すように、認証カード10B、11B、・・・、12Bとユーザ端末20Bとカードリーダー30Bとから構成されている。カードリーダー30Bとユーザ端末20Bとは、ケーブル40Bにて接続されている。

【0108】

認証カード10B、11B、・・・、12Bは、訪問業者より利用者宅へ訪問する訪問者一人一人に割り当てられており、割り当てられた訪問者のバイオメトリックス情報を身元証明鍵として予め記憶している。ここで、バイオメトリックス情報は訪問者の指紋模様の特徴点からなる身元証明指紋情報とする。つまり、認証カード10B、11B、・・・、12Bには、それぞれ異なる身元証明鍵が記憶されていることになる。

【0109】

カードリーダー30Bは、訪問者より指紋の入力を受け付ける指紋読取部310Bを有している。

ここでは、認証カード10Bとユーザ端末20Bとカードリーダー30Bとを用いて、身元認証システム1Bの概要について説明する。なお、認証カード11B、・・・、12Bは、認証カード10Bと同様であるため、説明は省略する。

【0110】

身元認証システム1Bは、認証カード10Bがカードリーダー30Bに挿入されると、訪問者に対して指紋の入力を要求する。身元認証システム1Bは、カードリーダー30Bの指紋読取部310Bより指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報と認証カード10Bに記憶している身元証明鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行い、認証結果をユーザ端末20Bの表示部203Bにて表示する。

【0111】

ここで用いる暗号処理は、身元認証システム1と同様に秘密鍵による暗号処理である。また、身元認証システム1と同様に身元証明鍵と身元認証指紋情報とが同一の鍵となることは、言うまでもない。

また、身元認証システム1Bにおいて、認証カード11B、・・・、12Bのうち何れかの認証カードがカードリーダー30Bに挿入された場合も同様の動作を行うため、説明は省略する。

【0112】

3. 2 認証カード10B

ここでは、認証カード10Bの構成について説明する。認証カード10Bは、ICを内蔵している可搬型の記録媒体であり、一例として、ICカード機能付メモリカードである。認証カード10Bは、図16に示すように、証明鍵記憶部101B、制御部102B及び入出力部103Bから構成されている。

【0113】

認証カード10Bは、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード10Bは、その機能を達成する。

なお、認証カード11B、・・・、12Bは、認証カード10Bと同様の構成を有しているため、説明は省略する。

【0114】

(1) 証明鍵記憶部101B

証明鍵記憶部101Bは、耐タンパ性を有しており、訪問者に対応する身元証明指紋情

報を身元証明鍵として1つ記憶している。

以降の説明において、必要に応じて、身元証明鍵として「SK1」を用いて説明する。

(2) 制御部102B

制御部102Bは、第2の実施の形態にて示した認証カード10Aの制御部102Aと同様であるため、説明は省略する。

【0115】

(3) 入出力部103B

入出力部103Bは、第2の実施の形態にて示した認証カード10Aの入出力部103Aと同様であるため、説明は省略する。つまり、入出力部103Bは、第1の実施の形態にて示した認証カード10の入出力部103とも同様である。

3.3 ユーザ端末20Bの構成

ここでは、ユーザ端末20Bの構成について説明する。ユーザ端末20Bは、図17に示すように、認証鍵記憶部201B、認証部202B、表示部203B及び入出力部204Bとから構成されている。

【0116】

ユーザ端末20Bは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末20Bは、その機能を達成する。

【0117】

(1) 認証鍵記憶部201B

認証鍵記憶部201Bは、耐タンパ性を有しており、身元認証指紋情報を記憶する領域を備えている。

(2) 認証部202B

認証部202Bは、乱数を記憶する乱数記憶領域250Bを有している。

【0118】

認証部202Bは、カードリーダー30Bより入出力部204Bを介して、訪問者より入力された指紋から生成された身元認証指紋情報と、カードリーダー30Bに認証カード10Bが挿入されたことを検知した旨を示す検知情報とを受け取ると、受け取った身元認証指紋情報を認証鍵記憶部201Bへ書き込む。次に、認証部202Bは、乱数「N」を生成し、生成した乱数「N」を入出力部204Bを介してカードリーダー30Bへ出力し、生成した乱数「N」を乱数記憶領域250Bに記憶する。

【0119】

さらに、認証部202Bは、カードリーダー30Bより入出力部204Bを介して、暗号化情報Enc(SK1、N)を受け取ると、認証鍵記憶部201Bにて記憶している身元認証指紋情報を取得して、取得した身元認証指紋情報を用いて、暗号化情報Enc(SK1、N)の復号を行い、復号により得られた復号結果と、乱数記憶領域250Bにて記憶している乱数「N」とが一致するか否かを判断する。

【0120】

復号結果と乱数「N」とが一致する場合には、認証部202Bは、カードリーダー30Bに挿入された認証カードが正当な認証カードであると認証し、認証結果として訪問者が正当な訪問者である旨を示す正当訪問者情報を生成し、生成した正当訪問者情報を表示部203Bへ出力する。復号結果と乱数「N」とが一致しない場合には、認証部202Bは、カードリーダー30Bに挿入された認証カードが不正な認証カードであると認証し、認証結果として訪問者が不正な訪問者である旨を示す不正訪問者情報を生成し、生成した不正訪問者情報を表示部203Bへ出力する。さらに、認証部202Bは、認証鍵記憶部201Bにて記憶している身元認証指紋情報、及び乱数記憶領域250Bにて記憶している乱数「N」の消去を行う。

【0121】

(3) 表示部 203B

表示部 203B は、第 2 の実施の形態にて示したユーザ端末 20A の表示部 203A と同様であるため、説明は省略する。つまり、第 1 の実施の形態にて示したユーザ端末 20 の表示部 203 と同様である。

(4) 入出力部 204B

入出力部 204B は、第 2 の実施の形態にて示したユーザ端末 20A の入出力部 204A と同様であるため、説明は省略する。つまり、第 1 の実施の形態にて示したユーザ端末 20 の入出力部 204 と同様である。

【0122】

3. 4 カードリーダー 30B

カードリーダー 30B は、図 17 に示すように、カード読取部 301B、入出力部 302B、表示部 303B 及び指紋読取部 310B から構成されている。

カードリーダー 30B は、具体的には、マイクロプロセッサ、ROM、RAM などから構成されるコンピュータシステムである。前記 ROM には、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、カードリーダー 30B は、その機能を達成する。

【0123】

(1) カード読取部 301B

カード読取部 301B は、認証カード 10B が挿入されたことの検知を行う。カード読取部 301B は、認証カード 10B が挿入されたことを検知すると、指紋の入力を要求する要求情報を生成し、生成した要求情報を表示部 303B へ出力する。次に、カード読取部 301B は、指紋読取部 310B より身元認証指紋情報を受け取ると、検知情報を生成し、生成した検知情報と指紋読取部 310B より受け取った身元認証指紋情報とを入出力部 302B を介してユーザ端末 20B へ出力する。

【0124】

さらに、カード読取部 301B は、ユーザ端末 20B より入出力部 302B を介して、乱数「N」を受け取ると、受け取った乱数「N」を認証カード 10B へ出力する。カード読取部 301B は、認証カード 10B より暗号化情報 Enc (SK1, N) を受け取ると、受け取った暗号化情報 Enc (SK1, N) を入出力部 302B を介してユーザ端末 20B へ出力する。

【0125】

(2) 表示部 303B

表示部 303B は、例えば、ディスプレイを備え、カード読取部 301B より要求情報を受け取ると、受け取った要求情報を表示する。これにより、訪問者へ指紋の入力を促すことができる。

(3) 指紋読取部 310B

指紋読取部 310B は、指紋センサーから構成され、指紋センサーにより、訪問者の指紋模様を読み取り、読み取った指紋模様を用いて、指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報をカード読取部 301B へ出力する。

【0126】

ここで、指紋模様の特徴点とは、隆線の端点や分岐点の方向や位置関係である。

(4) 入出力部 302B

入出力部 302B は、第 2 の実施の形態にて示したカードリーダー 30A の入出力部 302A と同様であるため、説明は省略する。つまり、第 1 の実施の形態にて示したカードリーダー 30 の入出力部 302 と同様である。

【0127】

3. 5 身元認証処理の動作

ここでは、認証カード 10B がカードリーダー 30B に挿入されてからユーザ端末 20B にて認証を行うまでの処理である身元認証処理の動作について、図 18 に示す流れ図を用いて説明する。

カードリーダー 3 0 B は、認証カード 1 0 B が挿入されたことを検知すると（ステップ S 4 0 0）、要求情報を生成し、生成した要求情報を表示する（ステップ S 4 0 5）。次にカードリーダー 3 0 B は、訪問者より入力された指紋より身元認証指紋情報を生成し（ステップ S 4 1 0）、さらに、検知情報を生成し（ステップ S 4 1 5）、ステップ S 4 1 0 にて生成した身元認証指紋情報と、ステップ S 4 1 5 にて生成した検知情報とをユーザ端末 2 0 B へ出力する（ステップ S 4 2 0）。

【0 1 2 8】

ユーザ端末 2 0 B は、カードリーダー 3 0 B より身元認証指紋情報と検知情報とを受け取ると、受け取った身元認証指紋情報を認証鍵記憶部 2 0 1 B へ書き込む（ステップ S 4 2 5）。次に、ユーザ端末 2 0 B は、乱数「N」を生成し、生成した乱数「N」をカードリーダー 3 0 B へ出力し、さらに、生成した乱数「N」を乱数記憶領域 2 5 0 B に記憶する（ステップ S 4 3 0）。

【0 1 2 9】

カードリーダー 3 0 B は、ユーザ端末 2 0 B より乱数「N」を受け取ると、受け取った乱数「N」を認証カード 1 0 B へ出力する（ステップ S 4 3 5）。

認証カード 1 0 B は、カードリーダー 3 0 B より乱数「N」を受け取ると（ステップ S 4 4 0）、受け取った乱数「N」を証明鍵記憶部 1 0 1 B にて記憶している身元証明鍵を用いて暗号化して、暗号化情報を生成し、生成した暗号化情報をカードリーダー 3 0 B へ出力する（ステップ S 4 4 5）。

【0 1 3 0】

カードリーダー 3 0 B は、認証カード 1 0 B より暗号化情報を受け取ると、受け取った暗号化情報をユーザ端末 2 0 B へ出力する（ステップ S 4 5 0）。

ユーザ端末 2 0 B は、カードリーダー 3 0 B より暗号化情報を受け取ると、受け取った暗号化情報と認証鍵記憶部 2 0 1 B にて記憶している身元認証指紋情報とを用いて、認証処理を行う（ステップ S 4 5 5）。

【0 1 3 1】

3. 6 認証処理の動作

ここでは、身元認証処理のステップ S 4 5 5 にて行われる認証処理について、図 1 9 に示す流れ図を用いて説明する。

ユーザ端末 2 0 B は、認証カード 1 0 B よりカードリーダー 3 0 B を介して暗号化情報を受け取る（ステップ S 5 0 0）。次に、ユーザ端末 2 0 B は、身元認証指紋情報を認証鍵記憶部 2 0 1 B より取得する（ステップ S 5 0 5）。さらに、ユーザ端末 2 0 B は、取得した身元認証指紋情報を用いて、ステップ S 5 0 0 にて受け取った暗号化情報を復号する（ステップ S 5 1 0）。

【0 1 3 2】

次に、ユーザ端末 2 0 B は、復号して得られた復号結果と、身元認証処理のステップ S 4 3 0 にて乱数記憶領域 2 5 0 B に記憶した乱数「N」とが一致するか否かの判断を行う（ステップ S 5 1 5）。

一致すると判断する場合には（ステップ S 5 1 5 における「YES」）、正当訪問者情報を生成し、生成した正当訪問者情報を表示し（ステップ S 5 2 0）、認証鍵記憶部 2 0 1 B にて記憶している身元認証指紋情報及び乱数記憶領域 2 5 0 B にて記憶している乱数「N」を消去し（ステップ S 5 3 0）、処理を終了する。

【0 1 3 3】

一致しないと判断する場合には（ステップ S 5 1 5 における「NO」）、不正訪問者情報を生成し、生成した不正訪問者情報を表示し（ステップ S 5 2 5）、認証鍵記憶部 2 0 1 B にて記憶している身元認証指紋情報及び乱数記憶領域 2 5 0 B に記憶している乱数「N」を消去し（ステップ S 5 3 0）、処理を終了する。

4. 第 4 の実施の形態

ここでは、本発明に係る第 4 の実施の形態としての身元認証システム 1 C について説明する。

【0134】

身元認証システム1Cでは、以下の動作を行う。

訪問者が利用者宅へ訪問する前に、訪問に係る情報を利用者宅のユーザ端末へ送信し、送信した情報と同様の情報を認証カードへ記憶しておく。訪問時に、先ず、身元認証鍵として訪問者の生体科学的特徴を示すバイオメトリックス情報を用いて、認証カードが正当な認証カードであるか否かの認証を行い、正当な認証カードであると判断する場合に、訪問者による訪問が正しいものであるかを判断するために、認証カードにて記憶している訪問に係る情報と事前に送信した情報とが同一であるか否かを判断する。

【0135】**4. 1 身元認証システム1Cの概要**

身元認証システム1Cは、図20に示すように、認証カード10C、11C、・・・、12Cと、ユーザ端末20Cと、カードリーダー30Cと、配信装置50Cとから構成されている。カードリーダー30Cとユーザ端末20Cとは、ケーブル40Cにて接続されている。

【0136】

認証カード10C、11C、・・・、12Cは、訪問業者より利用者宅へ訪問する訪問者一人一人に割り当てられており、割り当てられた訪問者のバイオメトリックス情報を身元証明鍵として予め記憶している。ここで、バイオメトリックス情報は指紋模様の特徴点からなる身元証明指紋情報とする。つまり、認証カード10C、11C、・・・、12Cには、それぞれ異なる身元証明鍵が記憶されていることになる。

【0137】

カードリーダー30Cは、訪問者より指紋の入力を受け付ける指紋読取部310Cを有している。

ここで、図20には、図示していないが、ユーザ端末20Cと同様の構成を有するユーザ端末21C、・・・、22Cも配信装置50Cとインターネットを介して接続されている。また、ユーザ端末21C、・・・、22Cは、カードリーダー30Cと同様の構成を有するカードリーダー31C、・・・、32Cとそれぞれ接続されている。

【0138】

ここでは、認証カード10Cとユーザ端末20Cとカードリーダー30Cとを用いて、身元認証システム1Cの概要について説明する。なお、認証カード11C、・・・、12Cは、認証カード10Cと同様であり、ユーザ端末21C、・・・、22Cは、ユーザ端末20Cと同様であり、カードリーダー31C、・・・、32Cは、カードリーダー30Cと同様であるため、説明は省略する。

【0139】

身元認証システム1Cでは、訪問業者が利用者宅へ訪問する前に、訪問者による訪問の正当性を検証するために使用する認証用訪問鍵と証明用訪問鍵とを生成し、訪問時間帯を示す時間情報、訪問内容を示す内容情報及び認証用訪問鍵とからなる認証用訪問情報をユーザ端末20Cへインターネットを介して送信する。さらに、身元認証システム1Cでは、送信した認証用訪問情報と対応する証明用訪問情報を、認証用訪問情報を送信したユーザ端末と対応付けて認証カード10Cにて記憶する。ここで、証明用訪問情報は、訪問時間帯を示す証明用時間情報、訪問内容を示す証明用内容情報及び証明用訪問鍵からなる情報である。

【0140】

身元認証システム1Cは、認証カード10Cがカードリーダー30Cに挿入されると、訪問者に対して指紋の入力を要求する。身元認証システム1Cは、カードリーダー30Cの指紋読取部310Cより指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報と認証カード10Cに記憶している身元証明鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行う。ここで用いる暗号処理は、身元認証システム1と同様に秘密鍵による暗号処理である。また、身元認証システム1と同様に身元証明鍵と身元認証指紋情報とが同一の鍵と

なることは、言うまでもない。

【0141】

次に、身元認証システム1Cは、カードリーダー30Cに挿入された認証カードが正当な認証カードであると認証した場合には、証明用訪問情報の正当性を検証するために、認証用訪問鍵及び証明用訪問鍵とを基に、暗号処理を用いたチャレンジレスポンス方式による認証を行う。ここで用いる暗号処理は、秘密鍵による暗号処理であり、証明用訪問鍵と認証用訪問鍵とが同一の鍵となることは、言うまでもない。

【0142】

身元認証システム1Cは、上記認証にて、証明用訪問情報が正当であると認証した場合には、認証カード10Cにて記憶されている証明用訪問情報に含まれる訪問時間帯及び訪問内容と、事前に送信された認証用訪問情報に含まれる訪問時間帯及び訪問内容とがそれぞれ一致するか否かを判断し、判断結果をユーザ端末20Cの表示部203Cにて表示する。

【0143】

4. 2 配信装置50C

配信装置50Cは、訪問者が利用者宅へ訪問する前に、認証用訪問情報をユーザ端末20Cへ送信する装置であり、認証用訪問情報を送信する際には、訪問者に対応する認証カード10Cが配信装置50Cに装着されている。

配信装置50Cは、図21に示すように、端末情報記憶部506C、制御部502C、操作部503C、送信部504C及び出力部505Cから構成されている。

【0144】

配信装置50Cは、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、モデムなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、配信装置50Cは、その機能を達成する。

【0145】

(1) 端末情報記憶部506C

端末情報記憶部506Cは、耐タンパ性を有しており、利用者宅へ配布したユーザ端末を一意に識別する端末IDを記憶している。

なお、ここで記憶されている端末IDの個数は、配布したユーザ端末の数と同一となることは言うまでもない。

【0146】

(2) 制御部502C

制御部502Cは、操作部503Cより認証用訪問情報をユーザ端末20Cへ配信する旨の訪問用配信情報と、訪問時間帯及び訪問内容とを受け取ると、認証用訪問鍵及び証明用訪問鍵を生成する。さらに制御部502Cは、生成した認証用訪問鍵、受け取った訪問時間帯及び訪問内容を用いて認証用訪問情報を生成し、生成した認証用訪問情報をユーザ端末20Cへ送信する。また、制御部502Cは、受け取った訪問時間帯及び訪問内容及び生成した証明用訪問鍵とを用いて証明用訪問情報を生成する。さらに、制御部502Cは、ユーザ端末20Cを識別する端末IDを端末情報記憶部506Cより取得し、取得した端末IDと生成した証明用訪問情報とを対応付けて、出力部505Cを介して認証カード10Cへ出力する。

【0147】

(3) 操作部503C

操作部503Cは、操作者の操作により、訪問用配信情報と、訪問時間帯及び訪問内容とを受け付けると、受け付けた訪問用配信情報と訪問時間帯と訪問内容とを制御部502Cへ出力する。

なお、操作者は、利用者宅へ訪問する訪問者自身に限らず、訪問業者に属する者であればよい。

【0148】

(4) 送信部 504C

送信部 504C は、制御部 502C より受け取った情報をユーザ端末 20C へインターネットを介して出力する。

(5) 出力部 505C

出力部 505C は、制御部 502C より受け取った情報を認証カード 10C へ出力する。

【0149】

4. 3 認証カード 10C

ここでは、認証カード 10C の構成について説明する。認証カード 10C は、IC を内蔵している可搬型の記録媒体であり、一例として、IC カード機能付メモリカードである。認証カード 10C は、図 22 に示すように、証明鍵記憶部 101C、訪問鍵記憶部 105C、制御部 102C 及び入出力部 103C から構成されている。

【0150】

認証カード 10C は、具体的には、マイクロプロセッサ、ROM、RAM などから構成されるコンピュータシステムである。前記 ROM には、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード 10C は、その機能を達成する。

なお、認証カード 11C、・・・、12C は、認証カード 10C と同様の構成を有しているため、説明は省略する。

【0151】

(1) 証明鍵記憶部 101C

証明鍵記憶部 101C は、耐タンパ性を有しており、訪問者に対応する身元証明指紋情報を身元証明鍵として 1 つ記憶している。

以降の説明において、必要に応じて、身元証明鍵として「SK1」を用いて説明する。

(2) 訪問鍵記憶部 105C

訪問鍵記憶部 105C は、耐タンパ性を有しており、図 23 に一例として示すように、証明用訪問情報テーブル T300 を備えている。

【0152】

証明用訪問情報テーブル T300 は、端末 ID、証明用時間情報、証明用内容情報及び証明用訪問鍵からなる組を 1 以上記憶するための領域を備えている。

端末 ID は、利用者宅に配布したユーザ端末を識別する識別子である。例えば、端末 ID「T-ID1」は、ユーザ端末 20C を示し、端末 ID「T-ID2」は、ユーザ端末 21C（図 20 では図示せず）を示している。

【0153】

証明用時間情報は、訪問者が訪問する時間帯を示す情報であり、証明用内容情報は、訪問内容を示す情報であり、証明用訪問鍵は、訪問者による訪問の正当性を検証するために使用する鍵である。

(3) 制御部 102C

制御部 102C は、配信装置 50C より入出力部 103C を介して端末 ID と証明用訪問情報とを受け取ると、受け取った端末 ID と証明用訪問情報とを訪問鍵記憶部 105C へ書き込む。

【0154】

また、制御部 102C は、カードリーダー 30C より入出力部 103C を介して、第 1 乱数「N1」を受け取ると、証明鍵記憶部 101C より身元証明鍵「SK1」を取得し、取得した身元証明鍵「SK1」を用いて、カードリーダー 30C より受け取った第 1 乱数「N1」に対して暗号化を施し、第 1 暗号化情報 Enc (SK1, N1) を生成する。制御部 102C は、生成した暗号化情報を入出力部 103C を介してカードリーダー 30C へ出力する。

【0155】

さらに、制御部 102C は、カードリーダー 30C より入出力部 103C を介して端末 ID と第 2 乱数「N2」とを受け取ると、受け取った端末 ID に対応する証明用訪問情報を取得し、取得した証明用訪問鍵を一時的に記憶する。

また、制御部 102C は、取得した証明用訪問情報に含まれる証明用訪問鍵「V-Key1」を取得し、取得した証明用訪問鍵「V-Key1」を用いて、カードリーダー 30C より受け取った第 2 乱数「N2」に対して暗号化を施し、第 2 暗号化情報 Enc (V-Key1、N2) を生成する。制御部 102C は、生成した第 2 暗号化情報を入出力部 103C を介してカードリーダー 30C へ出力する。

【0156】

さらに、制御部 102C は、証明用訪問情報に含まれる証明用時間情報と証明用内容情報をユーザ端末 20C へ出力する旨を示す出力指示情報をカードリーダー 30C より受け取ると、一時的に記憶している証明用訪問情報に含まれる証明用時間情報と証明用内容情報とを取得し、取得した証明用時間情報と証明用内容情報とを入出力部 103C を介してカードリーダー 30C へ出力する。

【0157】

(4) 入出力部 103C

入出力部 103C は、第 3 の実施の形態にて示した認証カード 10B の入出力部 103B と同様であるため、説明は省略する。つまり、入出力部 103C は、第 1 の実施の形態にて示した認証カード 10 の入出力部 103、及び第 2 の実施の形態にて示した認証カード 10A の入出力部 103A と同様である。

【0158】

4. 4 ユーザ端末 20C の構成

ここでは、ユーザ端末 20C の構成について説明する。ユーザ端末 20C は、図 24 に示すように、認証鍵記憶部 201C、認証部 202C、表示部 203C、入出力部 204C、受信部 205C、訪問情報記憶部 206C 及び時計部 207C とから構成されている。

【0159】

ユーザ端末 20C は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記 ROM 又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末 20C は、その機能を達成する。

【0160】

また、上記の身元認証システム 1C の概要にて示したように、ユーザ端末 21C、・・・、22C は、ユーザ端末 20C と同様の構成であるため、説明は省略する。

(1) 認証鍵記憶部 201C

認証鍵記憶部 201C は、第 3 の実施の形態にて示したユーザ端末 20B の認証鍵記憶部 201B と同様であるため、説明は省略する。

【0161】

(2) 訪問情報記憶部 206C

訪問情報記憶部 206C は、耐タンパ性を有しており、配信装置 50C より送信された認証用訪問情報を記憶する領域を備えている。

(3) 受信部 205C

受信部 205C は、配信装置 50C よりインターネットを介して、認証用訪問情報を受信すると、受信した認証用訪問情報を訪問情報記憶部 206C へ書き込む。

【0162】

これにより、ユーザ端末 20C は、訪問業者による訪問に係る情報を事前に記憶することができる。

(4) 時計部 207C

時計部 207C は、時刻を計時する。

(5) 認証部 202C

認証部 202C は、乱数を記憶する乱数記憶領域 250C を有しており、さらに、ユーザ端末 20C の端末 ID をも予め記憶している。

【0163】

認証部 202C は、カードリーダー 30C より入出力部 204C を介して、訪問者より入力された指紋から生成された身元認証指紋情報と、カードリーダー 30C に認証カード 10C が挿入されたことを検知した旨を示す検知情報とを受け取ると、受け取った身元認証指紋情報を認証鍵記憶部 201C へ書き込む。次に、認証部 202C は、第 1 乱数「N1」を生成し、生成した第 1 乱数「N1」を入出力部 204C を介してカードリーダー 30C へ出力し、生成した第 1 乱数「N1」を乱数記憶領域 250C に記憶する。

【0164】

さらに、認証部 202C は、カードリーダー 30C より入出力部 204C を介して、第 1 暗号化情報 Enc (SK1、N1) を受け取ると、認証鍵記憶部 201C にて記憶している身元認証指紋情報を取得し、取得した身元認証指紋情報を用いて、第 1 暗号化情報 Enc (SK1、N1) の復号を行い、復号により得られた復号結果と、乱数記憶領域 250C にて記憶している第 1 乱数「N1」とが一致するか否かを判断する。

【0165】

復号結果と第 1 乱数「N1」とが一致しない場合には、認証部 202C は、カードリーダー 30C に挿入された認証カードが不正な認証カードであると認証し、認証結果として不正訪問者情報を生成し、生成した不正訪問者情報を表示部 203C へ出力する。さらに、認証部 202C は、認証鍵記憶部 201C にて記憶している身元認証指紋情報及び乱数記憶領域 250C にて記憶している第 1 乱数「N1」の消去を行う。

【0166】

復号結果と第 1 乱数「N1」とが一致する場合には、認証部 202C は、予め記憶している端末 ID を取得し、さらに、第 2 乱数「N2」を生成し、乱数記憶領域 250C に記憶している内容を第 1 乱数「N1」から生成した第 2 乱数「N2」へと更新する。次に、認証部 202C は、生成した第 2 乱数「N2」と取得した端末 ID とを入出力部 204C を介してカードリーダー 30C へ出力する。さらに、認証部 202C は、カードリーダー 30C より入出力部 204C を介して、第 2 暗号化情報 Enc (V-Key1、N2) を受け取ると、訪問情報記憶部 206C にて記憶している認証用訪問情報を取得する。認証部 202C は、受け取った第 2 暗号化情報 Enc (V-Key1、N2) を、取得した認証用訪問情報に含まれる認証用訪問鍵を用いて、第 2 暗号化情報 Enc (V-Key1、N2) の復号を行い、復号により得られた復号結果と、乱数記憶領域 250C にて記憶している第 2 乱数「N2」とが一致するか否かを判断する。

【0167】

一致しない場合には、認証部 202C は、カードリーダー 30C に挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示部 203C へ出力し、乱数記憶領域 250C にて記憶している第 2 乱数「N2」を消去する。

一致する場合には、出力指示情報を生成し、生成した出力指示情報を入出力部 204C を介してカードリーダー 30C へ出力する。さらに、認証部 202C は、カードリーダー 30C より入出力部 204C を介して、証明用時間情報と証明用内容情報とを受け取ると、次の動作を行う。認証部 202C は、訪問情報記憶部 206C にて記憶している認証用訪問情報を取得する。次に、受け取った証明用時間情報及び証明用内容情報と、取得した認証用訪問情報に含まれる時間情報及び内容情報とがそれぞれ一致するか否かの判断を行う。

【0168】

少なくとも何れかが一致しない場合には、認証部 202C は、カードリーダー 30C に挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示部 203C へ出力する。

それぞれが一致すると判断する場合には、時計部 207C より現在時刻を取得し、取得

した現在時刻が認証用時間情報にて示される訪問時間帯の範囲であるか否かを判断する。訪問時間帯の範囲でないと判断する場合には、認証部 202C は、カードリーダー 30C に挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示部 203C へ出力し、訪問情報記憶部 206C にて記憶している認証用訪問情報、及び乱数記憶領域 250C にて記憶している第 2 乱数「N2」を消去する。

【0169】

訪問時間帯の範囲であると判断する場合には、認証部 202C は、正当訪問者情報を生成し、生成した正当訪問者情報を表示部 203C へ出力し、訪問情報記憶部 206C にて記憶している認証用訪問情報、及び乱数記憶領域 250C にて記憶している第 2 乱数「N2」を消去する。

(6) 表示部 203C

表示部 203C は、第 3 の実施の形態にて示したユーザ端末 20B の表示部 203B と同様であるため、説明は省略する。つまり、第 1 の実施の形態にて示したユーザ端末 20 の表示部 203、及び第 2 の実施の形態にて示したユーザ端末 20A の表示部 203A と同様である。

【0170】

(7) 入出力部 204C

入出力部 204C は、第 3 の実施の形態にて示したユーザ端末 20B の入出力部 204B と同様であるため、説明は省略する。つまり、第 1 の実施の形態にて示したユーザ端末 20 の入出力部 204、及び第 2 の実施の形態にて示したユーザ端末 20A の入出力部 204A と同様である。

【0171】

4. 5 カードリーダー 30C

カードリーダー 30C は、図 24 に示すように、カード読取部 301C、入出力部 302C、表示部 303C 及び指紋読取部 310C から構成されている。

カードリーダー 30C は、具体的には、マイクロプロセッサ、ROM、RAM などから構成されるコンピュータシステムである。前記 ROM には、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、カードリーダー 30C は、その機能を達成する。

【0172】

なお、上記の身元認証システム 1C の概要にて示したように、カードリーダー 31C、
・ ・ ・、32C は、カードリーダー 30C と同様の構成であるため、説明は省略する。

(1) カード読取部 301C

カード読取部 301C は、認証カード 10C が挿入されたことの検知を行う。カード読取部 301C は、認証カード 10C が挿入されたことを検知すると、指紋の入力を要求する要求情報を生成し、生成した要求情報を表示部 303C へ出力する。次に、カード読取部 301C は、指紋読取部 310C より身元認証指紋情報を受け取ると、検知情報を生成し、生成した検知情報と指紋読取部 310C より受け取った身元認証指紋情報とを入出力部 302C を介してユーザ端末 20C へ出力する。

【0173】

カード読取部 301C は、ユーザ端末 20C より入出力部 302C を介して、第 1 乱数「N1」を受け取ると、受け取った第 1 乱数「N1」を認証カード 10C へ出力する。カード読取部 301C は、認証カード 10C より第 1 暗号化情報 Enc (SK1、N1) を受け取ると、受け取った第 1 暗号化情報 Enc (SK1、N1) を入出力部 302C を介してユーザ端末 20C へ出力する。

【0174】

カード読取部 301C は、入出力部 302C を介してユーザ端末 20C より端末 ID と第 2 乱数「N2」とを受け取ると、受け取った端末 ID と第 2 乱数「N2」とを認証カード 10C へ出力する。さらに、カード読取部 301C は、認証カード 10C より第 2 暗号

化情報 Enc (V-Key 1、N2) を受け取ると、受け取った第2暗号化情報 Enc (V-Key 1、N2) を入出力部 302C を介してユーザ端末 20C へ出力する。

【0175】

カード読取部 301C は、入出力部 302C を介してユーザ端末 20C より出力指示情報を受け取ると、受け取った出力指示情報を認証カード 10C へ出力する。さらに、カード読取部 301C は、認証カード 10C より認証用時間情報及び認証用内容情報を受け取ると、受け取った認証用時間情報及び認証用内容情報を入出力部 302C を介してユーザ端末 20C へ出力する。

【0176】

(2) 表示部 303C

表示部 303C は、第3の実施の形態で示したカードリーダー 30B の表示部 303B と同様であるため、説明は省略する。

(3) 指紋読取部 310C

指紋読取部 310C は、第3の実施の形態で示したカードリーダー 30B の指紋読取部 310B と同様であるため、説明は省略する。

【0177】

(4) 入出力部 302C

入出力部 302C は、第3の実施の形態にて示したカードリーダー 30B の入出力部 302B と同様であるため、説明は省略する。つまり、第1の実施の形態にて示したカードリーダー 30 の入出力部 302、及び第2の実施の形態にて示したカードリーダー 30A の入出力部 302A と同様である。

【0178】

4.6 訪問情報配信処理の動作

ここでは、認証用訪問情報を事前に配信する訪問情報配信処理について、図25に示す流れ図を用いて、説明する。

配信装置 50C は、利用者の操作により、認証用訪問情報をユーザ端末 20C へ配信する旨の訪問用配信情報と、訪問時間帯及び訪問内容とを受け付けると (ステップ S600)、認証用訪問鍵及び証明用訪問鍵とを生成する (ステップ S605)。次に、配信装置 50C は、生成した認証用訪問鍵と、ステップ S600 にて受け取った訪問時間帯及び訪問内容とを用いて認証用訪問情報を生成し、生成した認証用訪問情報をユーザ端末 20C へ送信する (ステップ S610)。ユーザ端末 20C は、配信装置 50C より認証用訪問情報を受信すると (ステップ S615)、受信した認証用訪問情報を訪問情報記憶部 206C へ書き込む (ステップ S620)。

【0179】

配信装置 50C は、さらに、ステップ S605 にて生成した証明用訪問鍵と、ステップ S600 にて受け取った訪問時間帯及び訪問内容とを用いて証明用訪問情報を生成し、生成した証明用訪問情報を認証カード 10C へ出力する (ステップ S625)。

認証カード 10C は、証明用訪問情報を受け取ると、受け取った証明用訪問情報を訪問鍵記憶部 105C へ書き込む (ステップ S630)。

【0180】

4.7 身元認証処理の動作

ここでは、カードリーダー 30C に挿入された認証カード 10C の認証を行う処理である身元認証処理の動作について、図26及び図27に示す流れ図を用いて、説明する。

カードリーダー 30C は、認証カード 10C が挿入されたことを検知すると (ステップ S650)、要求情報を生成し、生成した要求情報を表示する (ステップ S655)。次に、カードリーダー 30C は、訪問者より入力された指紋より身元認証指紋情報を生成し (ステップ S660)、さらに、検知情報を生成し (ステップ S665)、ステップ S660 にて生成した身元認証指紋情報と、ステップ S665 にて生成した検知情報とをユーザ端末 20C へ出力する (ステップ S670)。

【0181】

ユーザ端末20Cは、カードリーダー30Cより身元認証指紋情報と検知情報とを受け取ると、受け取った身元認証指紋情報を認証鍵記憶部201Cへ書き込む（ステップS675）。次に、ユーザ端末20Cは、第1乱数「N1」を生成し、生成した第1乱数「N1」をカードリーダー30Cへ出力し、さらに、生成した第1乱数「N1」を乱数記憶領域250Cに記憶する（ステップS680）。

【0182】

カードリーダー30Cは、ユーザ端末20Cより第1乱数「N1」を受け取ると、受け取った第1乱数「N1」を認証カード10Cへ出力する（ステップS685）。

認証カード10Cは、カードリーダー30Cより第1乱数「N1」を受け取ると（ステップS690）、受け取った第1乱数「N1」を証明鍵記憶部101Cにて記憶している身元証明鍵を用いて暗号化して、第1暗号化情報を生成し、生成した第1暗号化情報をカードリーダー30Cへ出力する（ステップS695）。

【0183】

カードリーダー30Cは、認証カード10Cより第1暗号化情報を受け取ると、受け取った第1暗号化情報をユーザ端末20Cへ出力する（ステップS700）。

ユーザ端末20Cは、カードリーダー30Cより第1暗号化情報を受け取ると、受け取った第1暗号化情報と認証鍵記憶部201Cにて記憶している身元認証指紋情報とを用いて、認証処理を行う（ステップS705）。

【0184】

ユーザ端末20Cは、認証処理にて、カードリーダーに挿入された認証カードが正当な認証カードであると判断すると、端末IDを取得し（ステップS710）、さらに、第2乱数「N2」を生成し、乱数記憶領域250Cに記憶している内容を第1乱数「N1」から生成した第2乱数「N2」へと更新する（ステップS715）。次に、ユーザ端末20Cは、取得した端末IDと生成した第2乱数「N2」とをカードリーダー30Cへ出力する（ステップS720）。

【0185】

カードリーダー30Cは、ユーザ端末20Cより端末IDと第2乱数「N2」とを受け取ると、受け取った端末IDと第2乱数「N2」とを認証カード10Cへ出力する（ステップS725）。

認証カード10Cは、カードリーダー30Cより端末IDと第2乱数「N2」とを受け取ると（ステップS730）、受け取った端末IDに対応する証明用訪問情報を取得し、取得した証明用訪問情報を一時的に記憶する（ステップS735）。次に、認証カード10Cは、取得した証明用訪問情報に含まれる証明用訪問鍵を用いて暗号化して、第2暗号化情報を生成し、生成した第2暗号化情報をカードリーダー30Cへ出力する（ステップS740）。

【0186】

カードリーダー30Cは、認証カード10Cより第2暗号化情報を受け取ると、受け取った第2暗号化情報をユーザ端末20Cへ出力する（ステップS745）。

ユーザ端末20Cは、カードリーダー30Cより第2暗号化情報を受け取ると、受け取った第2暗号化情報と訪問情報記憶部206Cにて記憶している認証用訪問情報に含まれる認証用訪問鍵とを用いて、訪問鍵認証処理を行う（ステップS750）。

【0187】

ユーザ端末20Cは、訪問鍵認証処理にて、認証カード10Cに記憶されている証明用訪問情報が正当であると判断すると、出力指示情報を生成し、生成した出力指示情報をカードリーダー30Cへ出力する（ステップS755）。

カードリーダー30Cは、ユーザ端末20Cより出力指示情報を受け取ると、受け取った出力指示情報を認証カードへ出力する（ステップS760）。

【0188】

認証カード10Cは、カードリーダー30Cより出力指示情報を受け取ると、一時的に記憶している証明用訪問情報に含まれる証明用時間情報及び証明用内容情報を取得し、取得

した証明用時間情報及び証明用内容情報をカードリーダー30Cへ出力する（ステップS765）。

カードリーダー30Cは、認証カード10Cより証明用時間情報及び証明用内容情報を受け取ると、受け取った証明用時間情報及び証明用内容情報をユーザ端末20Cへ出力する（ステップS770）。

【0189】

ユーザ端末20Cは、カードリーダー30Cより証明用時間情報及び証明用内容情報を受け取ると、受け取った証明用時間情報及び証明用内容情報と、訪問情報記憶部206Cにて記憶している認証用訪問情報とを用いて、訪問情報検証処理を行う（ステップS775）。

4. 8 認証処理

図26にて示した身元認証処理のステップS705にて行われる認証処理について、図19にて示した認証処理との変更点を中心に説明する。

【0190】

先ず、ステップS515にて、肯定的に判断する場合（ステップS515における「YES」）、ステップS520以降は行わないで、図27に示すステップS710以降を行うように変更する。否定的に判断する場合は（ステップS515における「NO」）、図19に示す動作と同様である。なお、図27にて示す認証処理では、図19に示す乱数及び暗号化情報を、第1乱数及び第1暗号化情報と読み替える。

【0191】

4. 9 訪問鍵認証処理

ここでは、図27にて示した身元認証処理のステップS750にて行われる訪問鍵認証処理について、図28に示す流れ図を用いて説明する。

ユーザ端末20Cは、認証カード10Cよりカードリーダー30Cを介して、第2暗号化情報を受け取る（ステップS800）。次に、ユーザ端末20Cは、訪問情報記憶部206Cにて記憶している認証用訪問情報を取得し（ステップS805）、取得した認証用訪問情報に含まれる認証用訪問鍵を用いて、第2暗号化情報の復号を行い（ステップS810）、復号により得られた復号結果と、乱数記憶領域250Cにて記憶している第2乱数「N2」とが一致するか否かを判断する（ステップS815）。

【0192】

一致すると判断する場合には（ステップS815における「YES」）、図27にて示すステップS755以降を行う。

一致しないと判断する場合には（ステップS815における「NO」）、不正訪問者情報を生成し、生成した不正訪問者情報を表示部203Cへ出力し、乱数記憶領域250Cにて記憶している第2乱数「N2」を消去する（ステップS820）。

【0193】

4. 10 訪問情報検証処理

ここでは、図27にて示した身元認証処理のステップS775にて行われる訪問情報検証処理について、図29に示す流れ図を用いて説明する。

ユーザ端末20Cは、認証カード10Cよりカードリーダー30Cを介して、証明用時間情報及び証明用内容情報とを受け取る（ステップS850）。次に、ユーザ端末20Cは、訪問情報記憶部206Cにて記憶している認証用訪問情報を取得する（ステップS855）。

【0194】

ユーザ端末20Cは、取得した認証用訪問情報に含まれる認証用時間情報と証明用時間情報とが一致するか否かの判断、つまり事前に受信した訪問時間帯と認証カード10Cに記憶されている訪問時間帯とが一致するか否かの判断をする（ステップS860）。

時間帯が一致すると判断する場合には（ステップS860における「YES」）、取得した認証用訪問情報に含まれる認証用内容情報と証明用内容情報とが一致するか否かの判断、つまり事前に受信した訪問内容と認証カード10Cに記憶されている訪問内容とが一

致するか否かの判断をする（ステップ S 8 6 5）。

【0195】

訪問内容が一致すると判断する場合には（ステップ S 8 6 5 における「YES」）、時計部 2 0 7 C より現在の時刻を取得し（ステップ S 8 7 0）、取得した現在時刻が、認証用時間情報に示される時間帯の範囲内であるか否かを判断する（ステップ S 8 7 5）。

取得した現在時刻が、認証用時間情報に示される時間帯の範囲内であると判断する場合には（ステップ S 8 7 5 における「YES」）、正当訪問者情報を生成し、生成した正当訪問者情報を表示し（ステップ S 8 8 0）、訪問情報記憶部 2 0 6 C にて記憶している認証用訪問情報、及び乱数記憶領域 2 5 0 C にて記憶している第 2 乱数「N 2」を消去する（ステップ S 8 9 0）。

【0196】

時間帯が一致しないと判断する場合（ステップ S 8 6 0 における「NO」）、訪問内容が一致しないと判断する場合（ステップ S 8 6 5 における「NO」）、及び取得した現在時刻が認証用時間情報に示される時間帯の範囲内でないと判断する場合（ステップ S 8 7 5 における「NO」）のうち何れかの場合には、不正訪問者情報を生成し、生成した不正訪問者情報を表示し、訪問情報記憶部 2 0 6 C にて記憶している認証用訪問情報、及び乱数記憶領域 2 5 0 C にて記憶している第 2 乱数「N 2」を消去する（ステップ S 8 9 0）。

。

【0197】

5. まとめ

以上、説明したように、本発明によれば、身元認証システムは、認証カードとユーザ端末との間で認証を行っている。そのため、従来のようにネットワーク接続されたサーバを用いて認証を行う必要がない。つまり、ユーザ端末とサーバとが通信できないため、訪問者の身分の確認ができなくなるという問題は生じなくなる。

【0198】

また、認証を行う毎に、乱数を発生させているため、認証カードにて生成される暗号化情報は、認証を行う毎に異なる内容となる。そのため、通信経路盗聴による成りすまし攻撃に対する耐性が高くなる。

また、身元認証鍵を配信する場合には、利用者宅の訪問前に任意のタイミングで身元認証鍵を配信することができるため、身元認証鍵の配信によるネットワーク負荷を避けることができる。つまり、複数の利用者宅へ身元認証鍵を配信する際に、分散させて配信することが可能となる。

【0199】

（変形例）

上記に説明した第 1、第 2、第 3 及び第 4 の実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

（1）上記第 1、第 2、第 3 及び第 4 の実施の形態にて示した認証処理において、チャレンジレスポンス方式による認証方法として、秘密鍵暗号処理を用いたが、これに限定されない。他の暗号処理を用いたチャレンジレスポンス方式による認証方法でもよい。

【0200】

例えば、公開鍵暗号処理を用いたチャレンジレスポンス方式による認証、認証を行う毎に異なる電子署名を用いたチャレンジレスポンス方式による認証、固定の電子署名を用いたチャレンジレスポンス方式による認証などである。

（a）公開鍵暗号処理を用いる場合

ここでは、各実施の形態ごとに、公開鍵暗号処理を用いた場合の変形例について説明する。

【0201】

＜第 1 の実施の形態の変形例＞

公開鍵暗号処理を用いた場合の身元認証システムについて、第 1 の実施の形態と異なる

点を中心に説明する。ここで、公開鍵暗号処理は、一例として、RSAである。RSAについては、公知であるため、説明は省略する。

認証カード10は、身元証明鍵「SK1」を秘密鍵として、証明鍵IDと対応付けて記憶している。

【0202】

ユーザ端末20は、公開鍵である身元認証鍵と、身元認証鍵を識別する証明鍵IDとからなる組を複数記憶している。なお、以降では、身元証明鍵「SK1」に対応する公開鍵である身元認証鍵を「PK1」として説明を行う。

ユーザ端末20は、カードリーダー30より検知情報と証明鍵IDとを受け取ると、証明IDと一致する認証IDに対応付けられた身元認証鍵「PK1」を取得する。次に、ユーザ端末20は、乱数「N」を生成し、生成した乱数「N」を乱数記憶領域250に記憶し、さらに、生成した乱数「N」を取得した身元認証鍵「PK1」を用いて暗号化を行い、暗号化情報Enc(PK1、N)を生成し、生成した暗号化情報Enc(PK1、N)をカードリーダー30を介して認証カード10へ出力する。

【0203】

認証カード10は、ユーザ端末20より暗号化情報Enc(PK1、N)を受け取ると、受け取った暗号化情報Enc(PK1、N)を、記憶している身元証明鍵「SK1」を用いて、復号を行い、復号にて得られた復号結果をカードリーダー30を介してユーザ端末20へ出力する。

ユーザ端末20は、認証カード10より復号結果を受け取ると、受け取った復号結果と、記憶している乱数「N」とが一致するか否かを判断を行い、一致すると判断する場合には、カードリーダー30Aに挿入された認証カードが正当な認証カードであると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。一致しないと判断する場合には、カードリーダー30に挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。次に、ユーザ端末20は、乱数記憶領域250にて記憶している情報及びデータを消去する。

【0204】

<第2の実施の形態の変形例>

第2の実施の形態と異なる点を中心に説明する。認証カード10Aは、秘密鍵として身元証明鍵「SK1」を認証鍵記憶部201Aにて記憶している。また、ユーザ端末20Aは、事前に配信装置50Aより配信された公開鍵である身元認証鍵「PK1」を記憶している。認証時の動作について、以下に説明する。ユーザ端末20Aは、カードリーダー30Aより検知情報を受け取ると、身元認証鍵「PK1」を認証鍵記憶部201Aより取得する。次に、ユーザ端末20Aは、乱数「N」を生成し、生成した乱数「N」を乱数記憶領域250Aに記憶し、さらに、生成した乱数「N」を取得した身元認証鍵「PK1」を用いて暗号化を行い、暗号化情報Enc(PK1、N)を生成し、生成した暗号化情報Enc(PK1、N)をカードリーダー30Aを介して認証カード10Aへ出力する。以降は、上記で示した動作と同様であるため、説明は省略する。なお、認証処理の終了時は、乱数記憶領域250Aにて記憶している乱数「N」の消去及び認証鍵記憶部201Aにて記憶している身元認証鍵「PK1」の消去を行う。

【0205】

<第3の実施の形態の変形例>

第3の実施の形態と異なる点を中心に説明する。ここでは、公開鍵を自由に設定可能なID暗号を用いる。なお、ここで用いるID暗号は、ID情報に基づく公開鍵暗号処理である。この場合の具体例を以下に説明する。なお、ここでは、ID情報を指紋模様の特徴点からなる情報とする。また、ID情報に基づく公開鍵暗号処理については、公知技術であるため、説明は省略する。なお、A. Shamir 著による「Identity-Based cryptosystems and signature schemes.」(In Advances in Cryptology - CRYPTO'84, Springer-Verlag LNCS 196, 47-53, 1984.)にて

、ID情報に基く公開鍵暗号処理についての詳細な記述がある。

【0206】

身元認証システム1Bは、さらに、認証カード10Bの着脱が可能なサーバ装置を備え、サーバ装置は、カードリーダー30Bの指紋読取部310Bと同様の動作を行うサーバ用指紋読取部を有している。サーバ装置は、認証カード10Bが装着され、サーバ用指紋読取部より認証カード10Bを所有する訪問者の指紋模様を読み取り、読み取った指紋模様を用いて、指紋模様の特徴点からなる指紋情報を生成する。次に、生成した指紋情報と秘密鍵を生成するアルゴリズムとを用いて、生成した指紋情報に対応する秘密鍵である身元証明鍵「SK」を生成し、生成した身元証明鍵「SK」を認証カード10Bの証明鍵記憶部101Bへ書き込む。

【0207】

カードリーダー30Bは、認証カード10Bが挿入されたことを検知すると、要求情報を表示し、指紋読取部310Bより訪問者の指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報と検知情報とをユーザ端末20Bへ出力する。

ユーザ端末20Bは、カードリーダー30Bより身元認証指紋情報と検知情報とを受け取り、受け取った身元認証指紋情報と公開鍵を生成するアルゴリズムとを用いて、身元認証指紋情報に対応する公開鍵「PK」を生成する。さらに、ユーザ端末20Bは、乱数「N」をも生成し、生成した乱数「N」を乱数記憶領域250Bに記憶し、さらに、生成した乱数「N」を生成した公開鍵「PK」を用いて、暗号化情報Enc(PK, N)を生成し、生成した暗号化情報Enc(PK, N)をカードリーダー30Bを介して認証カード10Bへ出力する。以降は、上記で示した動作と同様であるため、説明は省略する。なお、認証処理の終了時は、乱数記憶領域250Bにて記憶している乱数「N」の消去を行う。

【0208】

これにより、バイオメトリックス情報と公開鍵暗号処理とを用いた認証方法が実現できる。

＜第4の実施の形態の変形例＞

上記で示した第3の実施の形態の変形例と同様であるため、説明は省略する。なお、カードリーダー30Cに挿入された認証カードが正当な認証カードであると認証した場合には、身元認証システム1Cは、訪問鍵認証処理以降の動作を行う。

【0209】

(b) 認証を行う毎に異なる電子署名を用いる場合

ここでは、各実施の形態ごとに、認証を行う毎に異なる電子署名を用いた場合の変形例について説明する。

＜第1の実施の形態の変形例＞

認証を行う毎に異なる電子署名を用いた場合の身元認証システムについて、第1の実施の形態と異なる点を中心に説明する。ここで、電子署名は、一例として、有限体上のエルガマル署名である。有限体上のエルガマル署名は公知であるので説明は省略する。

【0210】

認証カード10は、身元証明鍵「SK1」を秘密鍵として、証明鍵IDと対応付けて記憶している。

ユーザ端末20は、認証鍵記憶部201にて、公開鍵である身元認証鍵と、身元認証鍵を識別する認証鍵IDとからなる組を複数記憶している。なお、以降では、身元証明鍵「SK1」に対応する公開鍵である身元認証鍵を「PK1」として説明を行う。

【0211】

ユーザ端末20は、カードリーダー30より検知情報と証明鍵IDとを受け取ると、受け取った証明鍵IDをID記憶領域251に記憶する。次に、ユーザ端末20は、乱数「N」を生成し、生成した乱数「N」を乱数記憶領域250に記憶し、さらに、生成した乱数「N」をカードリーダー30を介して認証カード10へ出力する。

認証カード10は、ユーザ端末20より乱数「N」を受け取ると、記憶している身元証

明鍵「SK1」を用いて、受け取った乱数「N」の電子署名を生成し、生成した電子署名をカードリーダー30を介してユーザ端末20へ出力する。

【0212】

ユーザ端末20は、認証カード10より電子署名を受け取ると、ID記憶領域251にて記憶している証明鍵IDと一致する認証鍵IDに対応付けられた身元認証鍵「PK1」を認証鍵記憶部201より取得し、取得した身元認証鍵「PK1」と、乱数「N」とを用いて、受け取った電子署名の署名検証を行う。ここで、署名検証は、電子署名が正当なものであるか否かを検証するアルゴリズムである。正当な電子署名であると判断する場合には、カードリーダー30に挿入された認証カードが正当な認証カードであると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。不正な電子署名であると判断する場合には、カードリーダー30に挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。次に、ユーザ端末20は、乱数記憶領域250にて記憶している乱数「N」、及びID記憶領域251にて記憶している証明鍵IDをそれぞれ消去する。

【0213】

<第2の実施の形態の変形例>

第2の実施の形態と異なる点を中心に説明する。認証カード10Aは、秘密鍵である、訪問者に対応する身元証明鍵「SK1」を認証鍵記憶部201Aにて記憶している。また、ユーザ端末20Aは、事前に配信装置50Aより配信された公開鍵である身元認証鍵「PK1」を記憶している。認証時の動作について、以下に説明する。ユーザ端末20Aは、カードリーダー30Aより検知情報を受け取ると、乱数「N」を生成し、生成した乱数「N」を乱数記憶領域250Aに記憶し、さらに、生成した乱数「N」をカードリーダー30Aを介して認証カード10Aへ出力する。

【0214】

次に、上記で示した動作と同様に、認証カード10Aでは、乱数「N」の電子署名を生成して、生成した電子署名をユーザ端末20Aへ出力し、ユーザ端末20Aでは、事前に配信されている身元認証鍵と乱数「N」とを用いて、受け取った電子署名の署名検証を行う。以降は、上記と同様であるため、説明は省略する。なお、認証処理の終了時は、乱数記憶領域250Aにて記憶している乱数「N」の消去及び認証鍵記憶部201Aにて記憶している身元認証鍵「PK1」の消去を行う。

【0215】

<第3の実施の形態の変形例>

第3の実施の形態と異なる点を中心に説明する。ここでは、公開鍵を自由に設定可能なID署名を用いる。なお、ここで用いるID署名は、ID情報に基づく電子署名方式であり、ID情報は指紋模様の特徴点からなる情報とする。ID署名については、公知技術であるため、説明は省略する。なお、A. Shamir著による「Identity-Based cryptosystems and signature schemes.」(In Advances in Cryptology - CRYPTO'84, Springer-Verlag LNCS 196, 47-53, 1984.)にて、ID署名についての詳細な記述がある。

【0216】

ID署名を用いた場合の具体例を以下に説明する。

身元認証システム1Bは、さらに、認証カード10Bの着脱が可能なサーバ装置を備え、サーバ装置は、カードリーダー30Bの指紋読取部310Bと同様の動作を行うサーバ用指紋読取部を有している。サーバ装置は、認証カード10Bが装着され、サーバ用指紋読取部より認証カード10Bを所有する訪問者の指紋模様を読み取り、読み取った指紋模様を用いて、指紋模様の特徴点からなる指紋情報を生成する。次に、生成した指紋情報と秘密鍵を生成するアルゴリズムとを用いて、生成した指紋情報に対応する秘密鍵である身元証明鍵「SK」を生成し、生成した身元証明鍵「SK」を認証カード10Bの証明鍵記憶部101Bへ書き込む。

【0217】

カードリーダー30Bは、認証カード10Bが挿入されたことを検知すると、要求情報を表示し、指紋読取部310Bより訪問者の指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成し、生成した身元認証指紋情報と検知情報とをユーザ端末20Bへ出力する。

ユーザ端末20Bは、カードリーダー30Bより身元認証指紋情報と検知情報を受け取ると、受け取った身元認証指紋情報を認証鍵記憶部201Bへ書き込む。次に、ユーザ端末20Bは、乱数「N」を生成し、生成した乱数「N」をカードリーダー30Bを介して認証カード10Bへ出力し、生成した乱数「N」を乱数記憶領域250Bに記憶する。

【0218】

認証カード10Bは、ユーザ端末20Bより乱数「N」を受け取ると、記憶している身元証明鍵「SK」を用いて、受け取った乱数「N」の電子署名を生成し、生成した電子署名をカードリーダー30Bを介してユーザ端末20Bへ出力する。

ユーザ端末20Bは、認証カード10Bより電子署名を受け取ると、認証鍵記憶部201Bにて記憶している身元認証指紋情報を取得し、取得した身元認証指紋情報と公開鍵を生成するアルゴリズムとを用いて、身元認証指紋情報に対応する公開鍵「PK」を生成する。生成した身元認証鍵「PK」と、乱数「N」とを用いて、受け取った電子署名の署名検証を行う。

【0219】

以降は、上記と同様の動作であるため、説明は省略する。

＜第4の実施の形態の変形例＞

上記で示した第3の実施の形態の変形例と同様であるため、説明は省略する。なお、カードリーダー30Cに挿入された認証カードが正当な認証カードであると認証した場合には、身元認証システム1Cは、訪問鍵認証処理以降の動作を行う。

【0220】

(c) 固定の電子署名を用いる場合

ここでは、各実施の形態ごとに、固定の電子署名を用いた場合の変形例について説明する。

＜第1の実施の形態の変形例＞

固定の電子署名を用いた場合の身元認証システムについて、第1の実施の形態と異なる点を中心に説明する。ここで、電子署名は、一例として、有限体上のエルガマル署名である。有限体上のエルガマル署名は公知であるので説明は省略する。

【0221】

身元認証システム1は、さらに、認証カード10の着脱が可能なサーバ装置を備え、サーバ装置は、身元証明鍵として電子署名を生成する秘密鍵「SK」を証明鍵IDと対応付けて記憶している。認証カード10は、証明鍵IDと身元証明鍵とを記憶する代わりに、認証カード10を識別するため識別子「ID」を記憶している。

また、ユーザ端末20は、認証鍵IDと身元認証鍵とを記憶する代わりに、身元認証鍵として公開鍵「PK」を認証鍵IDと対応付けて認証鍵記憶部201にて記憶している。

【0222】

サーバ装置は、認証カード10が装着されると、認証カード10に記憶されている識別子「ID」を取得し、記憶している秘密鍵「SK」を用いて、取得した識別子「ID」の電子署名を生成し、生成した電子署名と秘密鍵「SK」と対応する証明鍵IDとを認証カード10に書き込む。

カードリーダー30は、認証カード10が挿入されたことを検知すると、認証カード10にて記憶している電子署名と証明鍵IDと識別子「ID」とを読み出し、読み出した電子署名と証明鍵IDと識別子「ID」とをユーザ端末20へ出力する。

【0223】

ユーザ端末20は、電子署名と証明鍵IDと識別子「ID」とを受け取ると、受け取った証明鍵IDと一致する認証鍵IDに対応する公開鍵「PK」を認証鍵記憶部201より

取得し、取得した公開鍵「PK」と、受け取った識別子「ID」とを用いて、受け取った電子署名の署名検証を行う。ここで、署名検証は、電子署名が正当なものであるか否かを検証するアルゴリズムである。正当な電子署名であると判断する場合には、カードリーダー30に挿入された認証カードが正当な認証カードであると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。不正な電子署名であると判断する場合には、カードリーダー30に挿入された認証カードが正当な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。

【0224】

<第2の実施の形態の変形例>

第2の実施の形態と異なる点を中心に説明する。身元認証システム1Aは、さらに、上記と同様の動作を行うサーバ装置を備える。配信装置50Aは、身元認証鍵を記憶及びユーザ端末20Aへ配信する代わりに、公開鍵「PK」を記憶、及びユーザ端末20Aへ配信する。認証カード10Aは、身元証明鍵を記憶する代わりに、認証カード10Aを識別するため識別子「ID」を記憶している。また、ユーザ端末20Aは、事前に配信装置50Aより配信された身元認証鍵を記憶する代わりに、事前に配信装置50Aより配信された公開鍵「PK」を記憶している。

【0225】

なお、認証時の動作については、上記と同様の動作であるため、説明は省略する。また、配信装置50Aとサーバ装置とは、同一の装置であってもよい。

<第3の実施の形態の変形例>

第3の実施の形態と異なる点を中心に説明する。ここでは、公開鍵を自由に設定可能なID署名を用いる。なお、ここで用いるID署名は、ID情報に基く電子署名であり、ID情報は、指紋模様の特徴点からなる情報とする。この場合の具体例を以下に説明する。

【0226】

身元認証システム1Bは、さらに、認証カード10Bの着脱が可能なサーバ装置を備え、サーバ装置は、カードリーダー30Bの指紋読取部310Bと同様の動作を行うサーバ用指紋読取部を有している。認証カード10Bは、証明鍵IDと身元証明鍵とを記憶する代わりに、認証カード10Bを識別するため識別子「ID」を記憶している。

サーバ装置は、認証カード10Bが装着され、サーバ用指紋読取部より認証カード10Bを所有する訪問者の指紋模様を読み取り、読み取った指紋模様を用いて、指紋模様の特徴点からなる指紋情報を生成する。次に、生成した指紋情報と秘密鍵を生成するアルゴリズムとを用いて、生成した指紋情報に対応する秘密鍵「SK」を生成する。さらに、サーバ装置は、挿入された認証カード10Bに記憶されている識別子「ID」を取得し、生成した秘密鍵「SK」を用いて、取得した識別子「ID」の電子署名を生成し、生成した電子署名を認証カード10Bに書き込む。

【0227】

カードリーダー30Bは、認証カード10Bが挿入されたことを検知すると、要求情報を表示し、指紋読取部310Bより訪問者の指紋の入力を受け付けると、受け付けた指紋より指紋模様の特徴点からなる身元認証指紋情報を生成する。さらに、認証カード10Bにて記憶している電子署名と識別子「ID」とを読み出し、読み出した電子署名と識別子「ID」と生成した身元認証指紋情報とをユーザ端末20Bへ出力する。

【0228】

ユーザ端末20Bは、カードリーダー30Bより電子署名と識別子「ID」と身元認証指紋情報とを受け取ると、受け取った身元認証指紋情報と公開鍵を生成するアルゴリズムとを用いて、身元認証指紋情報に対応する公開鍵「PK」を生成する。ユーザ端末20Bは、生成した公開鍵「PK」と、受け取った識別子「ID」とを用いて、受け取った電子署名の署名検証を行う。以降は、上記で示した動作と同様であるため、説明は省略する。

【0229】

<第4の実施の形態の変形例>

上記で示した第3の実施の形態の変形例と同様であるため、説明は省略する。なお、カ

ードリーダー30Cに挿入された認証カードが正当な認証カードであると認証した場合には、身元認証システム1Cは、訪問鍵認証処理以降の動作を行う。

(2) 上記第1、第2、第3及び第4の実施の形態において、認証方法をチャレンジレスポンス方式としたが、これに限定されない。他の認証方法を用いてもよい。

【0230】

例えば、一方向性の認証である。この場合の認証方法について、第1の実施の形態に基づいて、以下に説明する。

認証カード10は、カードリーダー30に挿入されると、乱数「N」を生成し、生成した乱数「N」に記憶している身元証明鍵「SK1」を用いて暗号化し、暗号化情報Enc (SK1, N) を生成する。次に、認証カード10は、生成した乱数「N」と暗号化情報Enc (SK1, N) とをカードリーダー30を介してユーザ端末20へ出力する。

【0231】

ユーザ端末20は、認証カード10より乱数「N」と暗号化情報Enc (SK1, N) とを受け取ると、受け取った暗号化情報Enc (SK1, N) を記憶している身元認証鍵「SK1」を用いて、復号する。ユーザ端末20は、復号して得られた復号結果と認証カード10より受け取った乱数「N」とが一致するか否かを判断し、一致すると判断する場合には、カードリーダー30に挿入された認証カードが正当な認証カードであると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。一致しないと判断する場合には、カードリーダー30に挿入された認証カードが不正な認証カードであると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。

【0232】

また、第2の実施の形態においては、認証カード10Aは、上記にて示した動作と同様の動作を行う。ユーザ端末20Aは、認証カード10Aより受け取った乱数「N」と暗号化情報Enc (SK1, N) と、配信装置50Aより事前に受け取り、記憶している身元認証鍵とを用いて、上記にて示した動作と同様の動作を行う。なお、認証後は、事前に記憶している身元認証鍵を消去する。

【0233】

また、第3の実施の形態においては、認証カード10Bは、上記にて示した動作と同様の動作を行う。ユーザ端末20Bは、認証カード10Bより受け取った乱数「N」と暗号化情報Enc (SK1, N) と、カードリーダー30Bより受け取った身元認証指紋情報とを用いて、上記にて示した動作と同様の動作を行う。

また、第4の実施の形態においては、認証カード10Cは、上記にて示した動作と同様の動作を行う。ユーザ端末20Cは、認証カード10Cより受け取った乱数「N」と暗号化情報Enc (SK1, N) と、カードリーダー30Cより受け取った身元認証指紋情報とを用いて、上記にて示した動作と同様の動作を行う。

【0234】

(3) 上記第1、第2、第3及び第4の実施の形態において、認証カードをカードリーダーへ挿入して、認証を行ったが、これに限定されない。

カードリーダーの表面にセンサー部を設け、認証カードをセンサー部へ接触させることにより認証を行ってもよい。

または、認証カードに無線タグを備え付け、センサー部とは非接触とすることによる認証を行ってもよい。

【0235】

(4) 上記第1、第2、第3及び第4の実施の形態において、ユーザ端末とカードリーダーとをケーブルにて接続したが、これに限定されない。

ユーザ端末とカードリーダーとを無線による通信にて接続してもよい。

(5) 上記第1、第2、第3及び第4の実施の形態において、認証結果をユーザ端末に表示したが、これに限定されない。

【0236】

認証により、正当な訪問者であると判断する場合には、玄関のドアの鍵を解除するよう

にしてもよい。この場合、玄関のドアは電子ロックにて鍵の施錠及び解除を行う。鍵の施錠及び解除を行う構成部を玄関制御部と呼ぶ。ユーザ端末は、カードリーダーに挿入された認証カードが正当な認証カードであると認証した場合には、正当訪問者情報を生成し、生成した正当訪問者情報を玄関制御部に出力し、カードリーダーに挿入された認証カードが不正な認証カードであると認証した場合には、不正訪問者情報を生成し、生成した不正訪問者情報を玄関制御部へ出力する。玄関制御部は、ユーザ端末より受け取った情報が正当訪問者情報及び不正訪問者情報のうち何れかであるかを判断し、正当訪問者情報であると判断する場合には、鍵の解除を行い、不正訪問者情報であると判断する場合には、鍵の解除を行わない。

【0237】

(6) ユーザ端末と認証カードとの通信方法は、上記第1、第2、第3及び第4の実施の形態にて示した通信方法に限定されない。他の通信方法を用いてもよい。

例えば、図30にて示す身元認証システム1Dの構成であってもよい。

身元認証システム1Dについて、一例として、第1の実施の形態と異なる点を中心に以下に説明する。

【0238】

(A) 身元認証システム1Dの概要

身元認証システム1Dは、認証カード10D、11D、・・・、12D、ユーザ端末20D、第1入出力装置60D及び認証カードの着脱可能な第2入出力装置70Dとから構成される。ここでは、身元認証システム1Dの概要について説明を認証カード10Dとユーザ端末20Dと第1入出力装置60Dと第2入出力装置70Dとを用いて行う。

【0239】

ユーザ端末20Dは、利用者の宅内に配置されており、第1入出力装置60Dは、利用者の宅外（例えば、玄関先）に配置されており、ユーザ端末20Dと第1入出力装置60Dとは、ケーブル40Dにて接続されている。

身元認証システム1Dは、認証カード10Dが第2入出力装置70Dに装着されると、第1入出力装置60Dと第2入出力装置70Dとの間にて情報の入出力を行うことにより、第1の実施の形態にて示した認証処理を行う。ここでは、第1入出力装置60Dと第2入出力装置70Dとの間における情報の入出力をQRコードからなる画像情報を用いて行う。画像情報のやりとりは、以下のようにして行う。ユーザ端末20Dが画像情報を受け取る場合には、第1入出力装置60Dの画像受取部601Dを用いて、第2入出力装置70Dの表示部703Dにて表示された画像情報を受け取る。また、認証カード10Dが画像情報を受け取る場合には、第2入出力装置70Dの画像受取部702Dを用いて、第1入出力装置60Dの表示部602Dにて表示された画像情報を受け取る。

【0240】

なお、身元認証システム1Dにおいて、認証カード11D、・・・、12Dが第2入出力装置70Dに装着された場合も同様の動作を行うため、説明は省略する。

(B) 認証カード10Dの構成

ここでは、認証カード10Dの構成について説明する。認証カード10Dは、ICを内蔵している可搬型の記録媒体であり、一例として、ICカード機能付メモ리카ードである。認証カード10Dは、図31に示すように、証明鍵記憶部101D、制御部102D及び入出力部103Dから構成されている。

【0241】

認証カード10Dは、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、認証カード10Dは、その機能を達成する。

なお、認証カード11D、・・・、12Dは、認証カード10Dと同様の構成を有しているため、説明は省略する。

【0242】

(a) 証明鍵記憶部 101D、入出力部 103D

証明鍵記憶部 101D 及び入出力部 103D は、それぞれ証明鍵記憶部 101 及び入出力部 103 と同様であるため、説明は省略する。

(b) 制御部 102D

制御部 102D は、第 2 入出力装置 70D より入出力部 103D を介して、証明鍵 ID を要求する旨の ID 要求情報を受け取ると、証明鍵記憶部 101D より証明鍵 ID を取得する。制御部 102D は、取得した証明鍵 ID を用いて、ID 用 QR コードを生成し、生成した ID 用 QR コードを入出力部 103D を介して第 2 入出力装置 70D へ出力する。

【0243】

さらに、制御部 102D は、第 2 入出力装置 70D より乱数「N」を示す乱数用 QR コードを受け取ると、受け取った乱数用 QR コードより乱数「N」を生成する。次に、制御部 102D は、証明鍵記憶部 101D より身元証明鍵「SK1」を取得し、取得した身元証明鍵「SK1」を用いて、乱数用 QR コードより生成した乱数「N」に対して暗号化を施し、暗号化情報 Enc (SK1、N) を生成する。制御部 102D は、生成した暗号化情報を暗号化用 QR コードを生成し、生成した暗号化用 QR コードを入出力部 103D を介して第 2 入出力装置 70D へ出力する。

【0244】

(C) 第 2 入出力装置 70D

ここでは、第 2 入出力装置 70D の構成について説明する。第 2 入出力装置 70D は、図 31 に示すように、カード読取部 701D、画像受取部 702D 及び表示部 703D から構成されている。

第 2 入出力装置 70D は、具体的には、マイクロプロセッサ、ROM、RAM などから構成されるコンピュータシステムである。前記 ROM には、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、第 2 入出力装置 70D は、その機能を達成する。

【0245】

(a) カード読取部 701D

カード読取部 701D は、認証カード 10D が装着されたことの検知を行う。カード読取部 701D は、認証カード 10D が挿入されたことを検知すると、ID 要求情報を生成し、生成した ID 要求情報を認証カード 10D へ出力する。次に、認証カード 10D より ID 用 QR コードを受け取ると、受け取った ID 用 QR コードを表示部 703D へ出力する。

【0246】

さらに、カード読取部 701D は、第 1 入出力装置 60D より画像受取部 702D を介して、乱数用 QR コードを受け取ると、受け取った乱数用 QR コードを認証カード 10D へ出力する。カード読取部 701D は、認証カード 10D より暗号化用 QR コードを受け取ると、受け取った暗号化用 QR コードを表示部 703D へ出力する。

(b) 画像受取部 702D

画像受取部 702D は、例えばカメラであり、第 1 入出力装置 60D にて表示されている画像を撮像し、撮像した画像をカード読取部 701D へ出力する。

【0247】

(c) 表示部 703D

表示部 703D は、例えばディスプレイであり、カード読取部 701D より受け取った情報を表示する。

(D) ユーザ端末 20D の構成

ここでは、ユーザ端末 20D の構成について説明する。ユーザ端末 20D は、認証カード 10D の認証を行う。ユーザ端末 20D は、図 32 に示すように、認証鍵記憶部 201D、認証部 202D、表示部 203D 及び入出力部 204D から構成されている。

【0248】

ユーザ端末 20D は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディ

スクユニット、ディスプレイユニットなどから構成されるコンピュータシステムである。前記ROM又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、ユーザ端末20Dは、その機能を達成する。

【0249】

(a) 認証鍵記憶部201D、表示部203D

認証鍵記憶部201D及び表示部203Dは、それぞれ認証鍵記憶部201及び表示部203と同様であるため、説明は省略する。

(b) 認証部202D

認証部202Dは、乱数を記憶する乱数記憶領域250D及び証明鍵IDを記憶するID記憶領域251Dを有している。

【0250】

認証部202Dは、第1入出力装置60Dより入出力部204Dを介して、ID用QRコードを受け取ると、受け取ったID用QRコードより証明鍵IDを生成し、生成した証明鍵IDをID記憶領域251Dに記憶する。次に、認証部202Dは、乱数「N」を生成し、生成した乱数「N」を乱数記憶領域250Dに記憶する。また、生成した乱数「N」を用いて、乱数用QRコードを生成し、生成した乱数用QRコードを入出力部204Dを介して第1入出力装置60Dへ出力する。さらに、認証部202Dは、第1入出力装置60Dより入出力部204Dを介して、暗号化用QRコードを受け取ると、受け取った暗号化用QRコードを用いて暗号化情報Enc(SK1、N)を生成する。次に、ID記憶領域251Dにて記憶している証明鍵IDと一致する認証鍵IDと対応する身元認証鍵を認証鍵記憶部201Dより取得し、取得した身元認証鍵を用いて、暗号化情報Enc(SK1、N)の復号を行い、復号により得られた復号結果と、乱数記憶領域250Dにて記憶している乱数「N」とが一致するか否かを判断する。一致すると判断する場合には、認証部202Dは、第2入出力装置70Dに装着されている認証カードが正当な認証カードであると認証し、正当訪問者情報を生成して、生成した正当訪問者情報を表示部203Dへ出力する。一致しないと判断する場合には、認証部202Dは、第2入出力装置70Dに装着されている認証カードが不正な認証カードであると認証し、不正訪問者情報を生成して、生成した不正訪問者情報を表示部203Dへ出力する。

【0251】

さらに、認証部202Dは、乱数記憶領域250Dに記憶している乱数「N」の消去、及びID記憶領域251Dに記憶している証明鍵IDの消去を行う。

(c) 入出力部204D

入出力部204Dは、第1入出力装置60Dより受け取った情報を認証部202Dへ出力し、認証部202Dから受け取った情報を第1入出力装置60Dへ出力する。

【0252】

(E) 第1入出力装置60D

ここでは、第1入出力装置60Dの構成について説明する。第1入出力装置60Dは、図32に示すように、画像受取部601D、表示部602D及び入出力部603Dから構成されている。

第1入出力装置60Dは、具体的には、マイクロプロセッサ、ROM、RAMなどから構成されるコンピュータシステムである。前記ROMには、コンピュータプログラムが記憶されている。前記マイクロプロセッサは、前記コンピュータプログラムに従って動作することにより、第1入出力装置60Dは、その機能を達成する。

【0253】

(a) 画像受取部601D

画像受取部601Dは、例えばカメラであり、第2入出力装置70Dにて表示されている画像を撮像し、撮像した画像を入出力部603Dを介してユーザ端末20Dへ出力する。

。

(b) 表示部602D

表示部 602D は、例えばディスプレイであり、入出力部 603D を介してユーザ端末 20D より受け取った情報を表示する。

【0254】

(F) 身元認証処理の動作

身元認証処理の動作は、第 1 の実施の形態にて示した身元認証処理の動作との変更点のみを説明する。まず、カードリーダー 30 にて行っていた動作を第 1 入出力装置 60D 及び第 2 入出力装置 70D にて行うことになる。第 1 入出力装置 60D と第 2 入出力装置 70D との情報の受け渡しは、それぞれに備えられた画像受取部を用いて、相手側装置に表示されている情報を撮像する。

【0255】

また、ユーザ端末 20D では、認証カード 10D へ出力する情報を QR コード化して出力するように変更し、認証カード 10D より受け取る情報は、QR コード化されているため QR コードより元の情報を生成して取得するように変更する。

認証カード 10D においてもユーザ端末 20D と同様に、ユーザ端末 20D へ出力する情報を QR コード化して出力するように変更し、ユーザ端末 20D より受け取る情報は、QR コード化されているため QR コードより元の情報を生成して取得するように変更する。

【0256】

(G) 認証処理の動作

認証処理の動作は、第 1 の実施の形態にて示した認証処理の動作との変更点のみを説明する。ステップ S100 を、認証カード 10D より暗号化用 QR コードを受け取り、受け取った暗号化用 QR コードから暗号化情報を生成し、取得するように変更する。

(H) 他の実施例への適用

これまで、第 1 の実施の形態と異なる点を中心に身元認証システム 1D の説明を行ったが、身元認証システム 1D にて用いた QR コードによる情報の受け渡しは第 2、第 3 及び第 4 の実施の変形例として適用できる。

【0257】

つまり、身元認証システムは、訪問者は利用者宅へ訪問した際に受け渡しされる情報を QR コード化して、QR コード化した情報の受け渡しを行えばよい。

なお、第 3 の実施の変形例として適用する場合には、第 2 入出力装置に、指紋読取部 310B と同様の指紋読取部を備えることで、実現できる。また、第 4 の実施の変形例として適用する場合にも、同様に第 2 入出力装置に、指紋読取部を備えることで、実現できる。

【0258】

(7) 上記 (6) では、QR コードを用いたが、他の画像情報であってもよい。例えば、バーコードである。

また、画像情報以外のものであってもよい。例えば、光信号である。

(8) 上記 (6) では、情報の受け渡しを、ディスプレイによる表示とカメラによる画像の撮像により行ったが、これに限定されない。

【0259】

例えば、第 1 及び第 2 入出力装置に赤外線機能を設けて、赤外線通信による情報の受け渡しを行ってもよい。このとき通信に用いられる信号は赤外線信号である。

または、第 1 及び第 2 入出力装置にスピーカとマイクとを設けて、受け渡しを行う情報を音声信号に変換して、変換した音声信号による通信を行ってもよい。

(9) 上記 (6) において、情報の受け渡しに第 1 及び第 2 入出力装置を用いたが、これに限定されない。

【0260】

例えば、第 1 入出力装置が有する機能をユーザ端末に設けて、第 2 入出力装置を認証カードの着脱が可能なカメラ付携帯電話機としてもよい。このとき、情報の受け渡しは、玄関ののぞき穴を利用して行われる。

(10) 上記(6)において、ユーザ端末20Dから認証カード10Dへ情報を出力する方法と、認証カード10D及び第2入出力装置70Dからユーザ端末20Dへ情報を出力する方法を同一の方法としたが、これに限定されない。ユーザ端末20Dから認証カード10Dへ情報を出力する方法と、認証カード10D及び第2入出力装置70Dからユーザ端末20Dへ情報を出力する方法とをそれぞれ異なる方法としてもよい。

【0261】

例えば、ユーザ端末20Dから認証カード10Dへ情報を出力する方法としてQRコードを用い、認証カード10D及び第2入出力装置70Dからユーザ端末20Dへ情報出力する方法として、音声信号を用いる。

(11) 上記第1、第2、第3及び第4の実施の形態において、ユーザ端末から認証カードへ出力する情報、認証カード及びカードリーダーからユーザ端末へ出力する情報をそれぞれ他の情報に変換して出力してもよい。

【0262】

例えば、ユーザ端末から認証カードへ出力する情報をQRコード化して、認証カードへ出力してもよい。このとき、認証カードは、ユーザ端末よりカードリーダーを介してQRコード化された情報を受け取ると、受け取ったQRコード化された情報を用いて、元の情報を生成することになる。また、同様に、認証カード及びカードリーダーからユーザ端末へ出力する情報をQRコード化して、ユーザ端末へ出力してもよい。このとき、ユーザ端末は、認証カードよりカードリーダーを介してQRコード化された情報やカードリーダーよりQRコード化された情報を受け取ると、受け取ったQRコード化された情報を用いて、元の情報を生成することになる。

【0263】

なお、上記に例では、ユーザ端末から情報を出力する方法と、認証カード及びカードリーダーから情報を出力する方法とを同一の方法(QRコード化した情報を出力する方法)としたが、ユーザ端末から情報を出力する方法と、認証カード及びカードリーダーから情報を出力する方法とをそれぞれ異なる方法としてもよい。

例えば、ユーザ端末から情報を出力する方法としてQRコードを用いて、認証カード及びカードリーダーから情報を出力する方法として音声信号を用いる。

【0264】

(12) 上記第1、第2、第3及び第4の実施の形態において、認証カードに制御部を設けたが、これに限定されない。認証カードに制御部を設けなくて、カードリーダーに制御部を設けて、認証カード内で行っていた処理をカードリーダーにて行ってもよい。

また、上記(6)においても同様に、認証カードに制御部を設けなくて、第2入出力装置に制御部を設けて、認証カード内で行っていた処理を第2入出力装置にて行ってもよい。

【0265】

(13) 上記第1、第2、第3及び第4の実施の形態及び上記(6)において、ユーザ端末を携帯電話機としてもよい。このとき、携帯電話機は、認証部を予め備えておいてもよいし、認証部と同様の動作を行うアプリケーションを訪問業者が有するアプリケーション配信装置よりダウンロードすることにより入手して、記憶してもよい。

または、インターホンやテレビドアホンにユーザ端末の機能を備えてもよい。

【0266】

(14) 上記第1、第2、第3及び第4の実施の形態及び上記(6)において、認証カードがユーザ端末を識別するようにしてもよい。

このとき、ユーザ端末は、端末IDを予め記憶しており、認証カードは、端末IDを記憶する記憶領域を備えている。ユーザ端末は、認証後、正当な訪問者であると判断する場合に、予め記憶している端末IDを認証カードへ出力する。認証カードは、受け取った端末IDを記憶領域へ記憶する。

【0267】

これにより、記憶領域に記憶された端末IDを訪問履歴として利用することができる。

(15) 上記第1、第2、第3及び第4の実施の形態及び上記(6)において、認証カードが、ユーザ端末を認証するようにしてもよい。

これにより、配達証明と同様のことが実現できる。

(16) 上記第1の実施の形態において、ユーザ端末20に記憶している身元認証鍵の変更及びユーザ端末20へ身元認証鍵の追加を行ってもよい。

【0268】

このとき、身元認証システム1は、さらに、配信装置を備え、配信装置は、ユーザ端末20へ、認証IDと身元認証鍵とからなる組を送信する。ユーザ端末20は、配信装置より、認証IDと身元認証鍵とからなる組を受信すると、受信した認証IDと一致する認証IDが鍵情報テーブルT100に存在するか否かを判断する。存在すると判断する場合には、受信した認証IDと一致する認証IDに対応する身元認証鍵を受信した身元認証鍵へと書き替える。存在しないと判断する場合には、新規の身元認証鍵として、受信した認証IDと身元認証鍵とからなる組を鍵情報テーブルT100に追加する。

【0269】

(17) 上記第2の実施の形態において、身元認証鍵を配信する場合には、配信する身元認証鍵を暗号化して配信してもよい。このとき、ユーザ端末は、暗号化された身元認証鍵を復号する復号鍵を、耐タンパ性を有する記憶領域にて予め記憶しており、受信した暗号化された身元認証鍵を復号鍵にて復号を行い、復号された身元認証鍵を、耐タンパ性を有する認証鍵記憶部にて記憶する。

【0270】

(18) 第2の実施の形態では、配信装置50Aとユーザ端末20Aをネットワーク接続する際にインターネットを利用したが、これに限定されない。専用線によるネットワーク接続であってもよい。

(19) 第2の実施の形態において、配信装置50Aより事前に配信され、記憶している身元認証鍵を認証後、消去したが、これに限定されない。

【0271】

認証後も、消去しないで記憶しておいてもよい。このとき、ユーザ端末20Aは、配信装置50Aより身元認証鍵を受け取ると、受け取った身元認証鍵と記憶している身元認証鍵とが一致するか否かを判断し、一致すると判断する場合には、鍵の書き換えは行わず、一致しないと判断する場合には、記憶している身元認証鍵から受け取った身元認証鍵へと書き換えを行う。

【0272】

(20) 上記第3の実施の形態において、認証に用いるバイオメトリックス情報として指紋模様の特徴点からなる情報(以下、単に「指紋情報」という。)を用いたが、これに限定されない。

バイオメトリックス情報として、例えば、指紋情報、訪問者の声紋の特徴を示す声紋情報、訪問者の虹彩の特徴を示す虹彩情報、訪問者の顔の輪郭の特徴を示す輪郭情報、訪問者のDNAの特徴を示すDNA情報又は、これら情報の組合せである。

【0273】

このとき、声紋情報を用いる場合は、カードリーダー30Bには、訪問者の音声を受け取り、受け取った音声から訪問者の声紋の特徴を示す身元認証声紋情報を生成する声紋読取部を設け、認証カード10Bには、訪問者の声紋の特徴を示す身元証明声紋情報を予め記憶しておく。

また、虹彩情報を用いる場合は、カードリーダー30Bには、訪問者の虹彩を読み取り、読み取った虹彩から訪問者の虹彩の特徴を示す身元認証虹彩情報を生成する虹彩読取部を設け、認証カード10Bには、訪問者の虹彩の特徴を示す身元証明虹彩情報を予め記憶しておく。

【0274】

また、輪郭情報を用いる場合は、カードリーダー30Bには、訪問者の顔の輪郭を読み取り、読み取った顔の輪郭から訪問者の顔の輪郭の特徴を示す身元認証輪郭情報を生成する

輪郭読取部を設け、認証カード10Bには、訪問者の顔の輪郭の特徴を示す身元証明輪郭情報を予め記憶しておく。

また、DNA情報を用いる場合は、カードリーダー30Bには、訪問者のDNAを解析したDNA情報である身元認証DNA情報を受け付けるDNA情報読取部を設け、認証カードには、訪問者のDNAを解析したDNA情報である身元証明DNA情報を予め記憶しておく。ここで、DNA情報とは、例えば、訪問者の髪の毛、血液又は唾液より解析される情報である。

【0275】

なお、第4の実施の形態においても同様に、バイオメトリックス情報を、例えば、指紋情報、訪問者の声紋の特徴を示す声紋情報、訪問者の虹彩の特徴を示す虹彩情報、訪問者の顔の輪郭の特徴を示す輪郭情報、訪問者のDNAの特徴を示すDNA情報又は、これら情報の組合せとしてもよい。

(21) 上記第3及び第4の実施の形態において、カードリーダーよりユーザ端末へ出力する身元認証指紋情報を暗号化して出力してもよい。

【0276】

このとき、カードリーダーは、身元認証指紋情報を暗号化する暗号鍵を予め記憶しており、また、ユーザ端末は、受け取った暗号化された身元認証指紋情報を復号する復号鍵を予め記憶することで実現できる。

(22) 上記第4の実施の形態にて示した訪問鍵認証処理において、チャレンジレスポンス方式による認証方法として、秘密鍵暗号処理を用いたが、これに限定されない。上記

(1)と同様に、他の暗号処理を用いたチャレンジレスポンス方式による認証方法でもよいし、上記(2)と同様に他の認証方法でもよい。

【0277】

(23) 上記(1)の(a)において、公開鍵をユーザ端末、秘密鍵を認証カードへそれぞれ記憶したが、これに限定されない。

公開鍵を認証カード、秘密鍵をユーザ端末へそれぞれ記憶してもよい。このときの認証の動作は、秘密鍵暗号処理を用いた場合と同様であるため、説明は省略する。

(24) 上記第1、第2、第3及び第4の実施の形態において、身元認証システムの構成要件であるユーザ端末とカードリーダーとをそれぞれ個別の装置として扱ったが、これに限定されない。

【0278】

ユーザ端末とカードリーダーとをユーザ端末とカードリーダーとからなる1つの装置として扱ってもよい。

また、上記(6)においても同様に、ユーザ端末と第1入出力装置とからなる1つの装置として扱ってもよい。

(25) 第4の実施の形態において、証明用訪問鍵と認証用訪問鍵とを基に認証を行う場合、第2乱数を生成して認証に使用したが、これに限定されない。第2乱数を生成しないで、先の認証にて使用した第1乱数を用いて、証明用訪問鍵と認証用訪問鍵とを基に認証を行ってもよい。このとき、図26及び図27にて示した身元認証処理においては、ステップS715を乱数記憶領域250Cにて記憶している第1乱数「N1」をカードリーダー30Cへ出力するように変更し、以下の動作にて第2乱数「N2」を用いる代わりに、第1乱数「N1」を用いて動作するように変更すればよい。

【0279】

(26) 第4の実施の形態において、認証用訪問鍵と証明用訪問鍵とを基にした認証後に、証明用時間情報及び証明用内容情報と、認証用訪問情報に含まれる時間情報及び内容情報とがそれぞれ一致するか否かの判断、及び訪問時間帯の判断を行ったが、これに限定されない。

認証用訪問鍵と証明用訪問鍵とを基にした認証を行わないで、つまり身元認証指紋情報と身元証明情報とを基にした認証後に、証明用時間情報及び証明用内容情報と、認証用訪問情報に含まれる時間情報及び内容情報とがそれぞれ一致するか否かの判断、及び訪問時

間帯の判断を行ってもよい。

【0280】

または、認証用訪問鍵と証明用訪問鍵とを基にした認証を行わないで、つまり身元認証指紋情報と身元証明情報とを基にした認証後に、証明用時間情報及び証明用内容情報と、認証用訪問情報に含まれる時間情報及び内容情報とがそれぞれ一致するか否かの判断のみ行ってもよいし、訪問時間帯の判断のみ行ってもよい。

または、身元認証指紋情報と身元証明情報とを基にした認証後に、認証用訪問鍵と証明用訪問鍵とを基にした認証のみを行ってもよい。

【0281】

(27) 上記第1、第2及び第3の実施の形態において、認証カードの証明鍵記憶部のみが耐タンパ性を有したが、他の構成要素においても耐タンパ性を有してもよい。

例えば、上記第1の実施の形態において、認証カード10の構成要素である証明鍵記憶部101、制御部102及び入出力部103の全てが耐タンパ性を有してもよい。

また、第4の実施の形態においても同様に、認証カードの証明鍵記憶部及び訪問鍵記憶部が耐タンパ性を有したが、他の構成要素においても耐タンパ性を有してもよい。

【0282】

(28) 上記第1、第2、第3及び第4の実施の形態において、ユーザ端末は、認証カードより受け取った暗号化情報(第4の実施の形態では、第1暗号化情報)を復号し、復号して得られた復号結果と、生成し記憶している乱数(第4の実施の形態では、第1乱数)とを用いて、復号結果と乱数(第4の実施の形態では、第1乱数)とが一致するか否かの判断を行ったが、これに限定されない。

【0283】

ユーザ端末は、生成し記憶している乱数(第4の実施の形態では、第1乱数)を用いて、記憶している身元認証鍵(第3及び第4の実施の形態では、身元認証指紋情報)を用いて暗号化して、暗号化乱数を生成し、生成した暗号化乱数と、認証カードより受け取った暗号化情報とを用いて、暗号化乱数と暗号化情報とが一致するか否かの判断を行い、一致する場合には、認証カードが正当な認証であると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。一致しない場合には、認証カードが不正な認証であると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。

【0284】

(29) 上記第1、第2、第3及び第4の実施の形態において、ユーザ端末は、生成した乱数(第4の実施の形態では、第1乱数)を認証カードへ出力したが、身元認証鍵(第3及び第4の実施の形態では、身元認証指紋情報)を用いて、乱数を暗号化して暗号化乱数を生成し、生成した暗号化乱数を出力してもよい。

このとき、認証カードでは、ユーザ端末より受け取った暗号化乱数を、身元証明鍵を用いて復号して得られた復号結果をユーザ端末へ出力し、ユーザ端末では、認証カードより受け取った復号結果と、記憶している乱数(第4の実施の形態では、第1乱数)とが一致するか否かの判断を行う。一致する場合には、認証カードが正当な認証であると認証し、正当訪問者情報を生成し、生成した正当訪問者情報を表示する。一致しない場合には、認証カードが不正な認証であると認証し、不正訪問者情報を生成し、生成した不正訪問者情報を表示する。

【0285】

(30) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0286】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【0287】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(31) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【産業上の利用可能性】**【0288】**

上記において説明した身元認証システムは、訪問業者による訪問者が利用者宅に訪問して、セールス、宅配サービス、その他サービスの提供などを行う産業において、経営的、つまり反復的かつ継続的に利用されうる。

【図面の簡単な説明】**【0289】**

【図1】 身元認証システム1の全体の概要を示す図である。

【図2】 認証カード10の構成を示すブロック図である。

【図3】 ユーザ端末20及びカードリーダー30の構成を示すブロック図である。

【図4】 認証鍵記憶部201が有する鍵情報テーブルT100のデータ構造を示す。

【図5】 身元認証システム1における身元認証処理の動作を示す流れ図である。

【図6】 身元認証システム1における認証処理の動作を示す流れ図である。

【図7】 身元認証システム1Aの全体の概要を示す図である。

【図8】 配信装置50Aの構成を示すブロック図である。

【図9】 配信鍵記憶部501Aが有する配信鍵情報テーブルT200のデータ構造を示す。

【図10】 認証カード10Aの構成を示すブロック図である。

【図11】 ユーザ端末20A及びカードリーダー30Aの構成を示すブロック図である。

。

【図12】 身元認証システム1Aにおける配信処理の動作を示す流れ図である。

【図13】 身元認証システム1Aにおける身元認証処理の動作を示す流れ図である。

【図14】 身元認証システム1Aにおける認証処理の動作を示す流れ図である。

【図15】 身元認証システム1Bの全体の概要を示す図である。

【図16】 認証カード10Bの構成を示すブロック図である。

【図17】 ユーザ端末20B及びカードリーダー30Bの構成を示すブロック図である。

。

【図18】 身元認証システム1Bにおける身元認証処理の動作を示す流れ図である。

【図19】 身元認証システム1Bにおける認証処理の動作を示す流れ図である。

【図20】 身元認証システム1Cの全体の概要を示す図である。

【図21】 配信装置50Cの構成を示すブロック図である。

【図22】 認証カード10Cの構成を示すブロック図である。

【図23】 訪問鍵記憶部105Cが有する証明用訪問情報テーブルT300のデータ構造を示す。

【図24】 ユーザ端末20C及びカードリーダー30Cの構成を示すブロック図である。

。

【図25】 身元認証システム1Cにおける訪問情報配信処理の動作を示す流れ図である。

【図 2 6】身元認証システム 1 C における身元認証処理の動作を示す流れ図である。
図 2 7 へ続く。

【図 2 7】身元認証システム 1 C における身元認証処理の動作を示す流れ図である。
図 2 6 から続く。

【図 2 8】身元認証システム 1 C における訪問鍵認証処理の動作を示す流れ図である。

【図 2 9】身元認証システム 1 C における訪問情報検証処理の動作を示す流れ図である。

【図 3 0】身元認証システム 1 D の全体の概要を示す図である。

【図 3 1】認証カード 1 0 D 及び第 2 入出力装置 7 0 D の構成を示すブロック図である。

【図 3 2】ユーザ端末 2 0 D 及び第 1 入出力装置 6 0 D の構成を示すブロック図である。

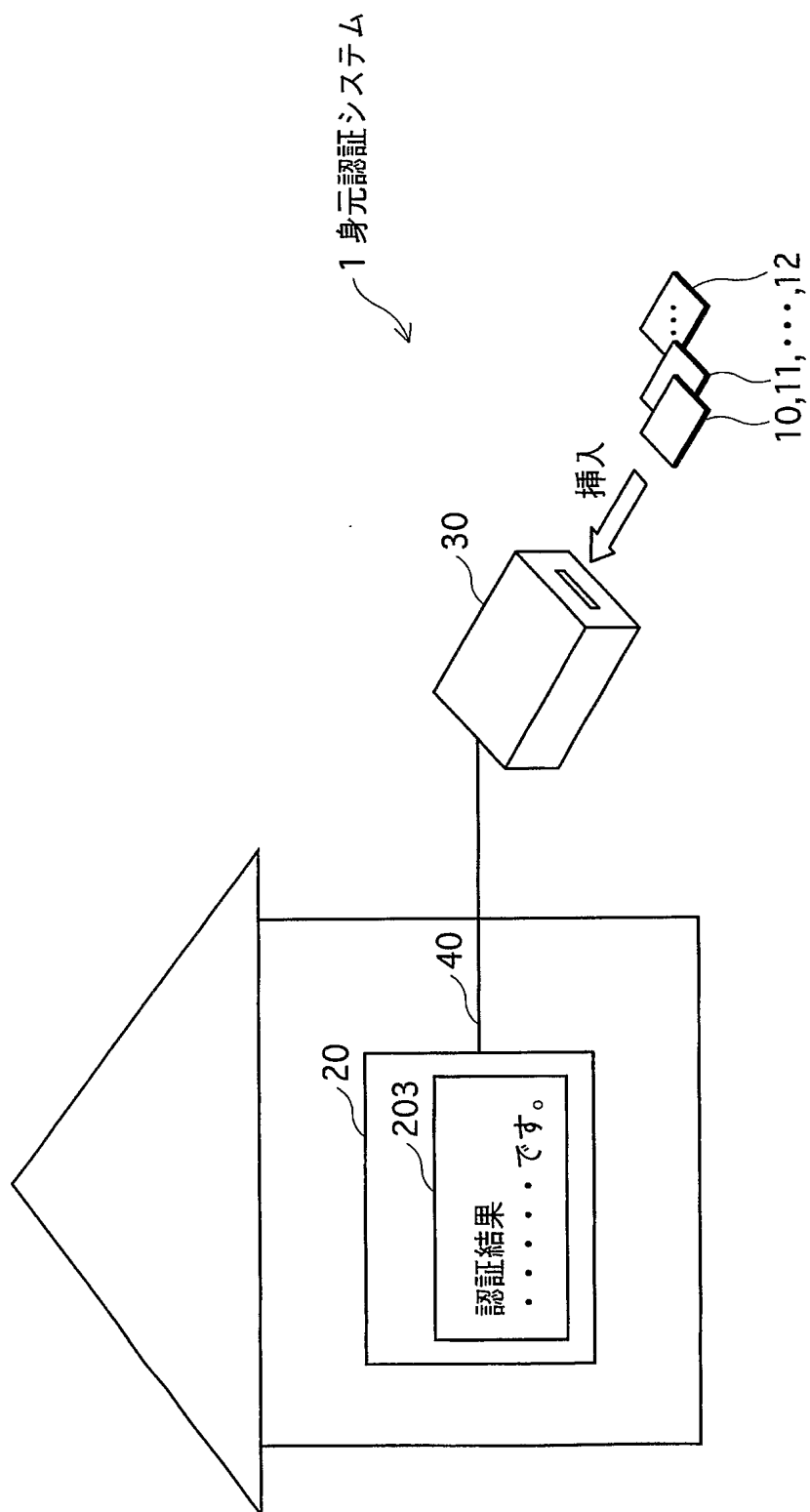
【符号の説明】

【0 2 9 0】

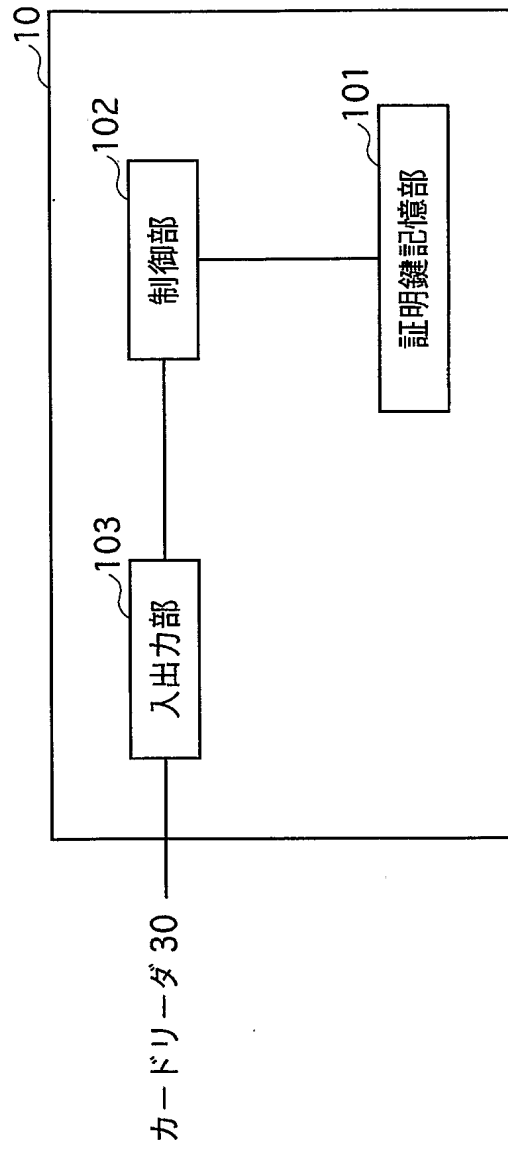
- 1 身元認証システム
- 1 0 ~ 1 2 認証カード
- 2 0 ユーザ端末
- 3 0 カードリーダー
- 4 0 ケーブル
- 1 0 1 証明鍵記憶部
- 1 0 2 制御部
- 1 0 3 入出力部
- 2 0 1 認証鍵記憶部
- 2 0 2 認証部
- 2 0 3 表示部
- 2 0 4 入出力部
- 2 5 0 乱数記憶領域
- 2 5 1 I D 記憶領域
- 3 0 1 カード読取部
- 3 0 2 入出力部
- 3 0 3 表示部

【書類名】 図面

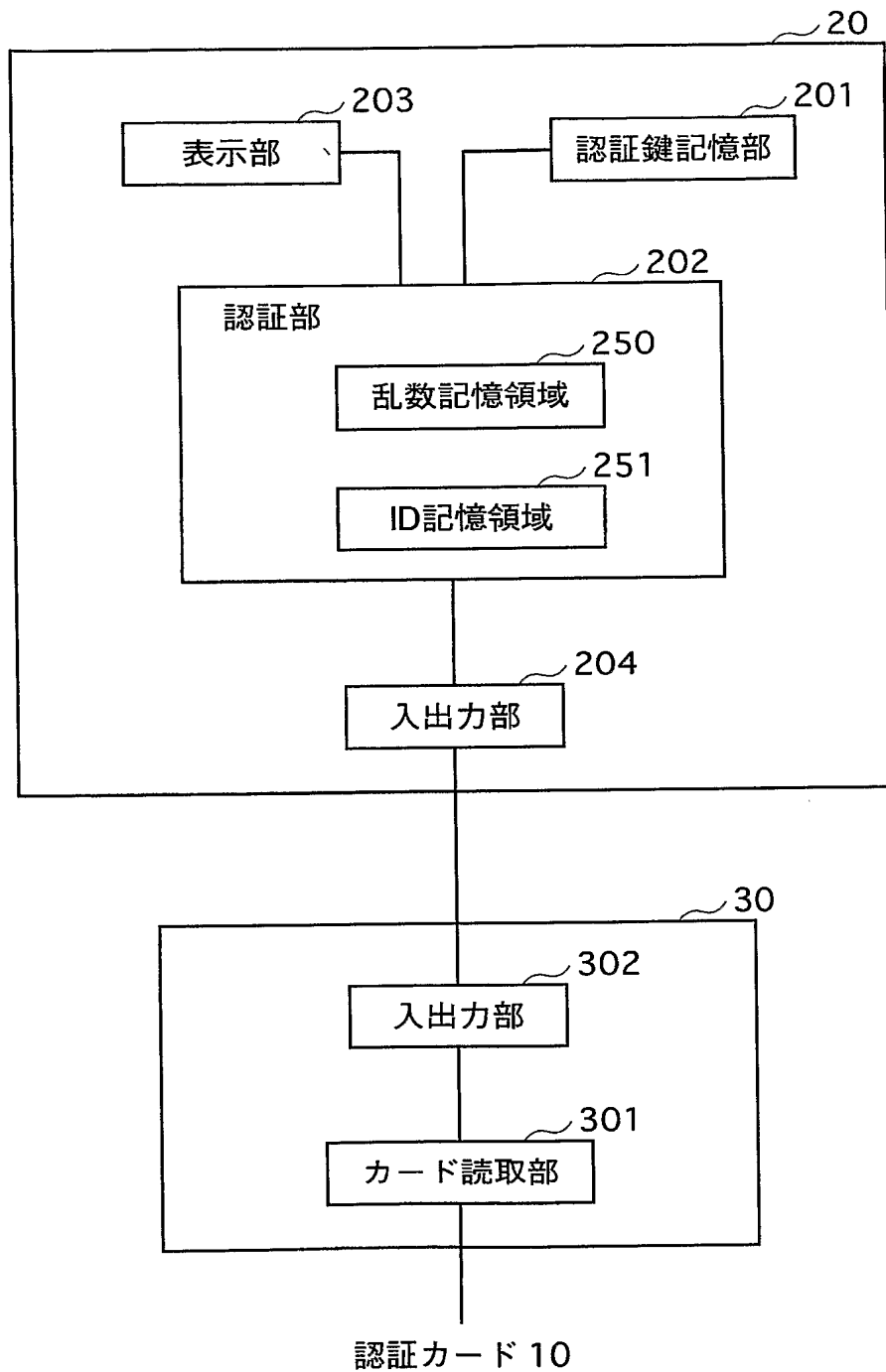
【図 1】



【図 2】



【図 3】

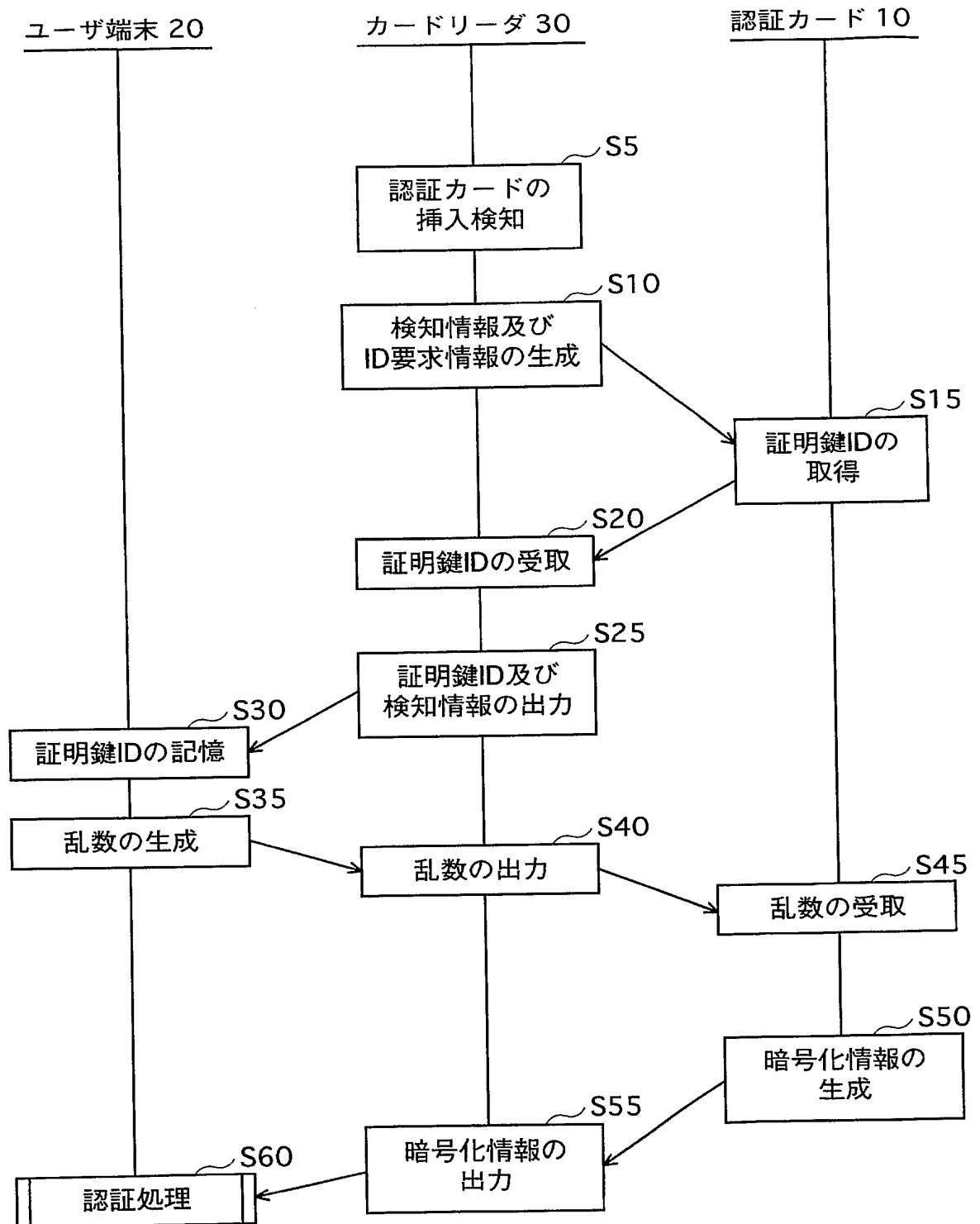


【図 4】

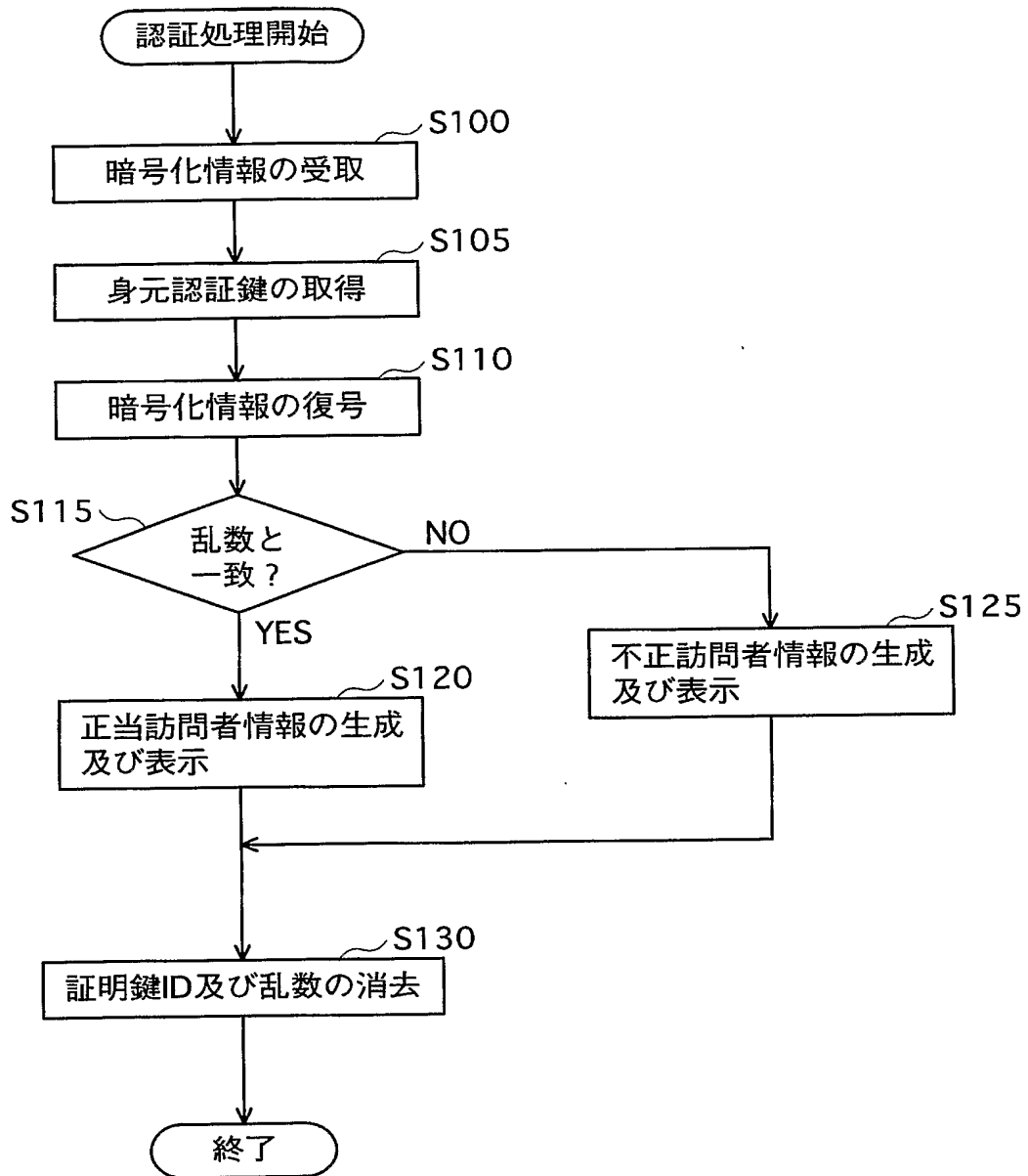
T100
↙

認証鍵ID	身元認証鍵
ID 1	SK 1
ID 2	SK 2
ID 3	SK 3
⋮	⋮
⋮	⋮
⋮	⋮

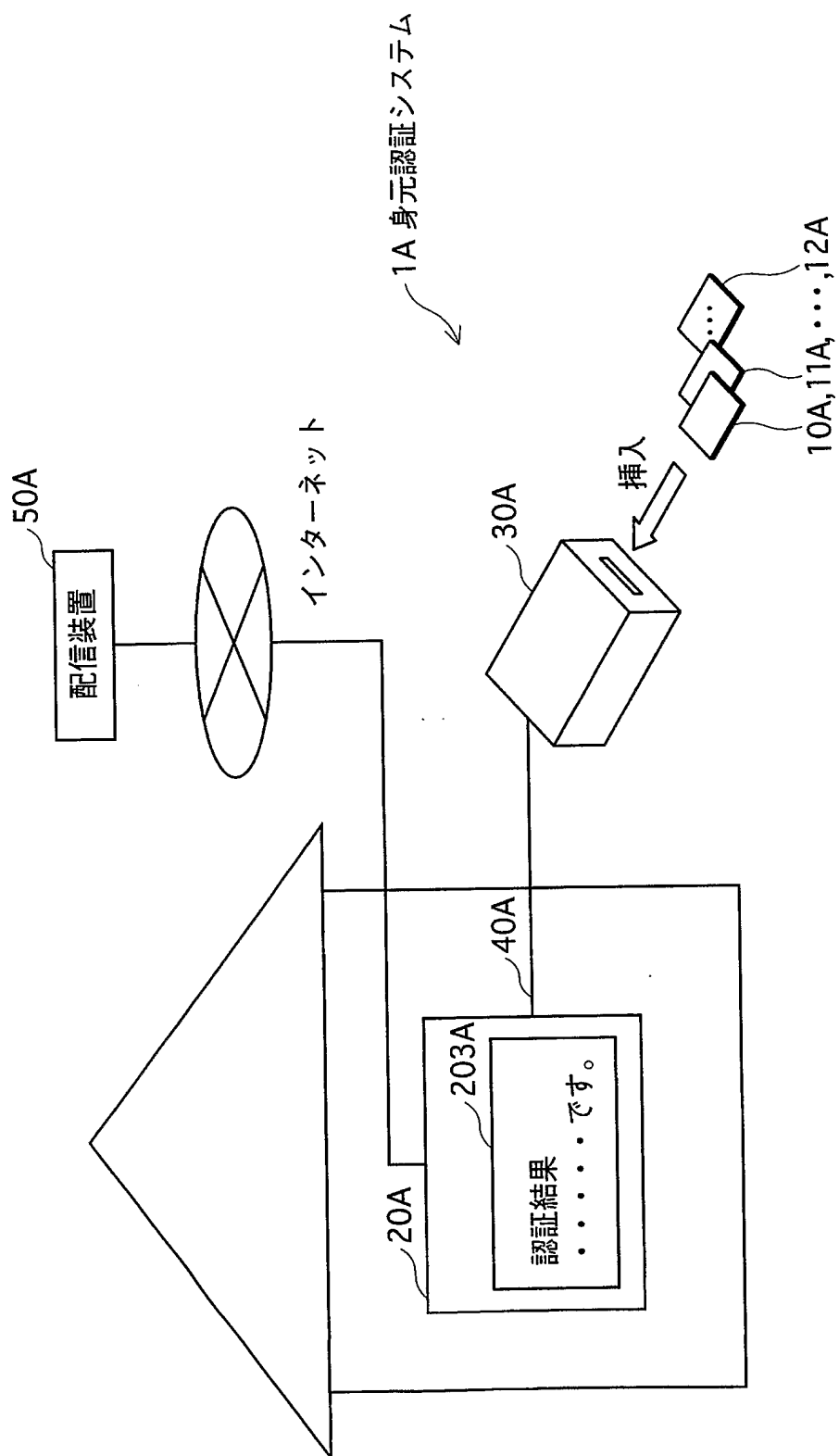
【図 5】



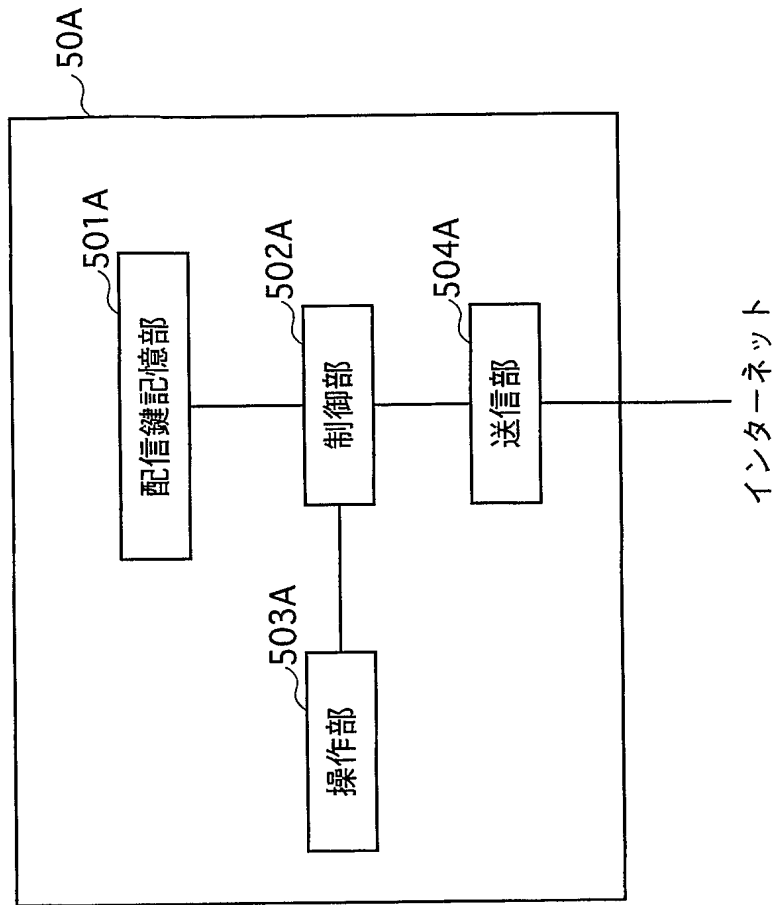
【図 6】



【図 7】



【図 8】

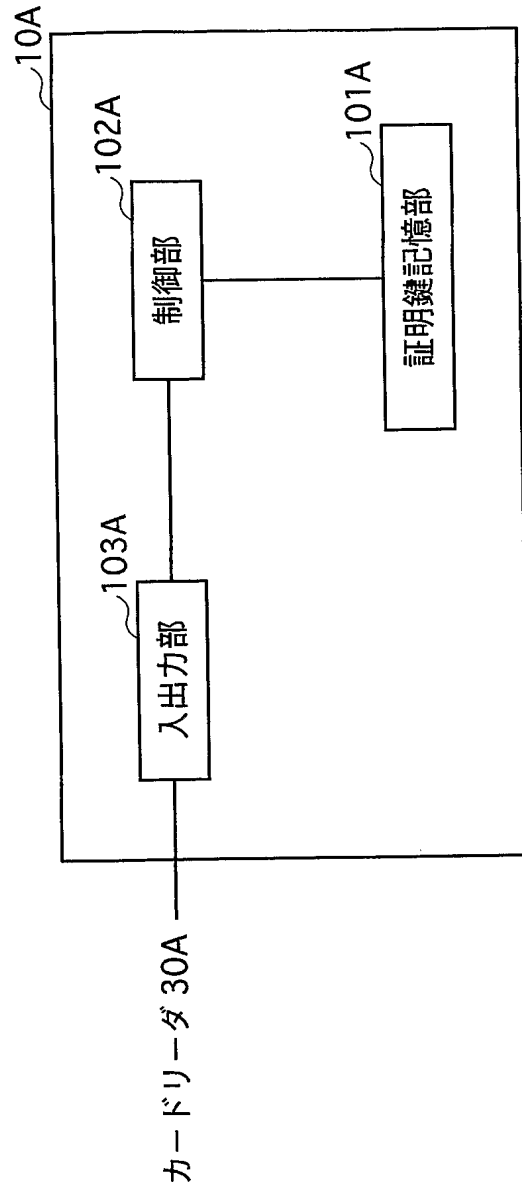


【図 9】

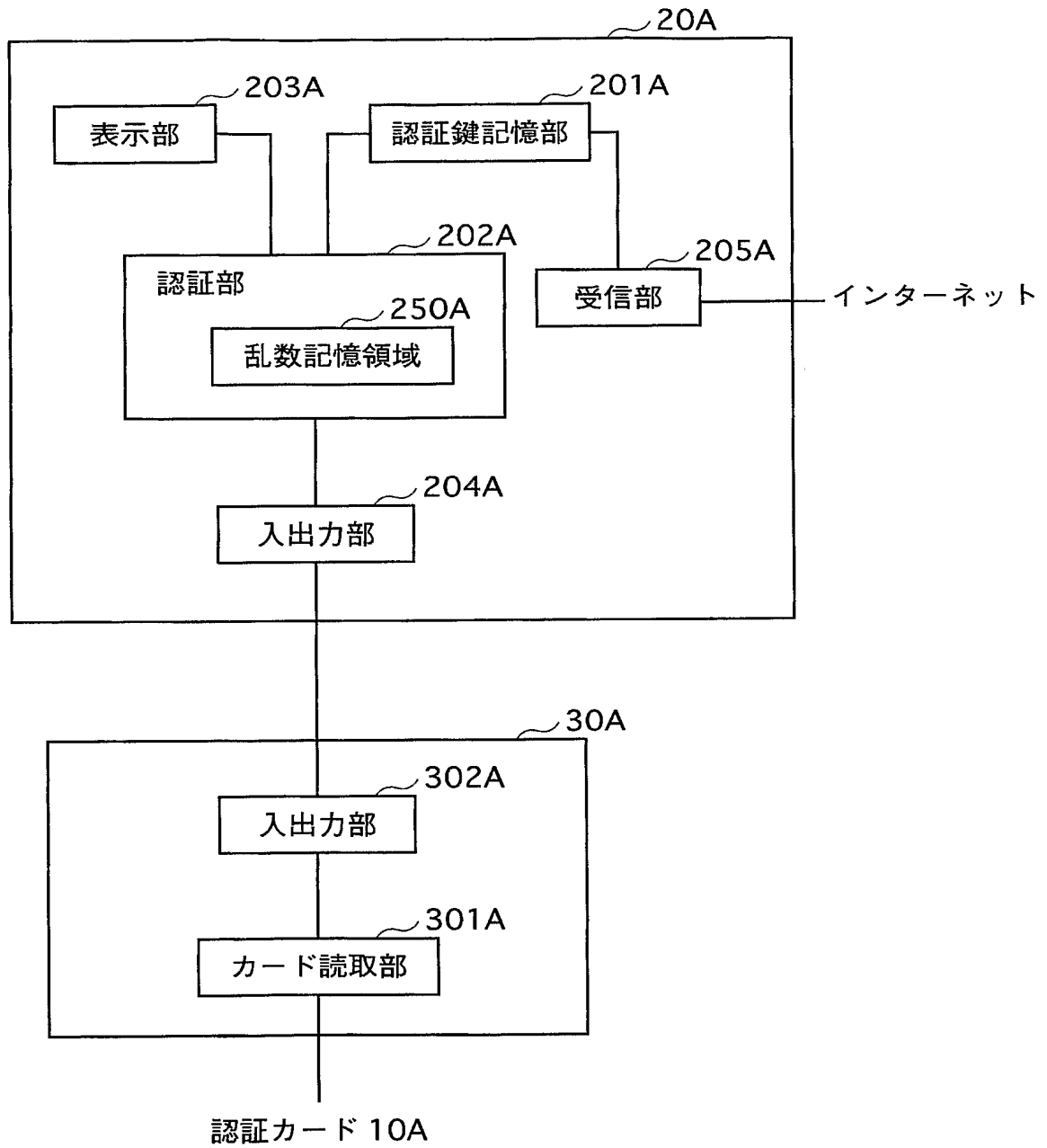
T200
↙

訪問者ID	身元認証鍵
VID 1	SK 1
VID 2	SK 2
⋮	⋮

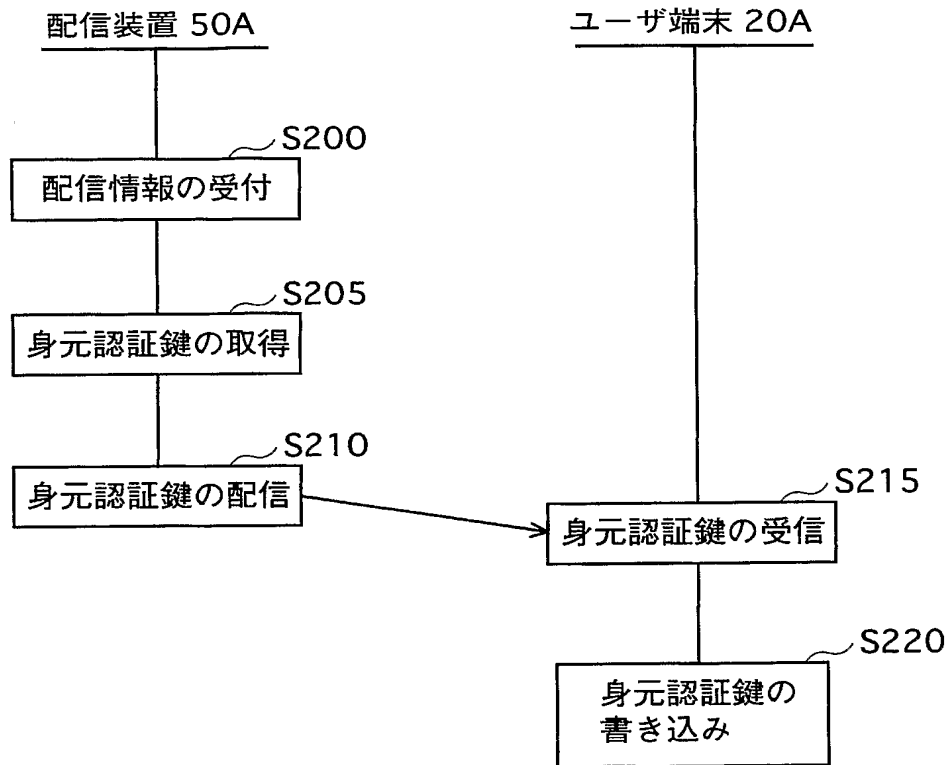
【図 10】



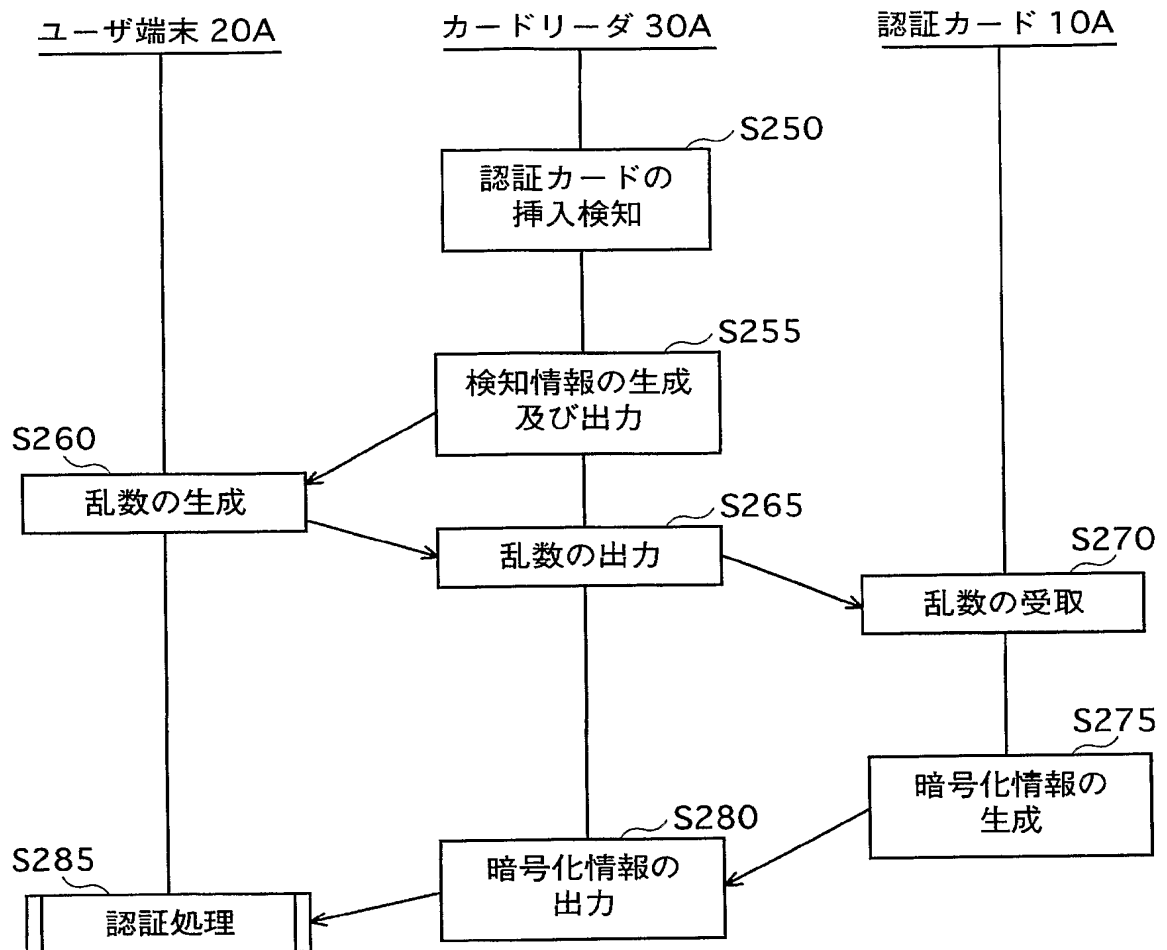
【図 11】



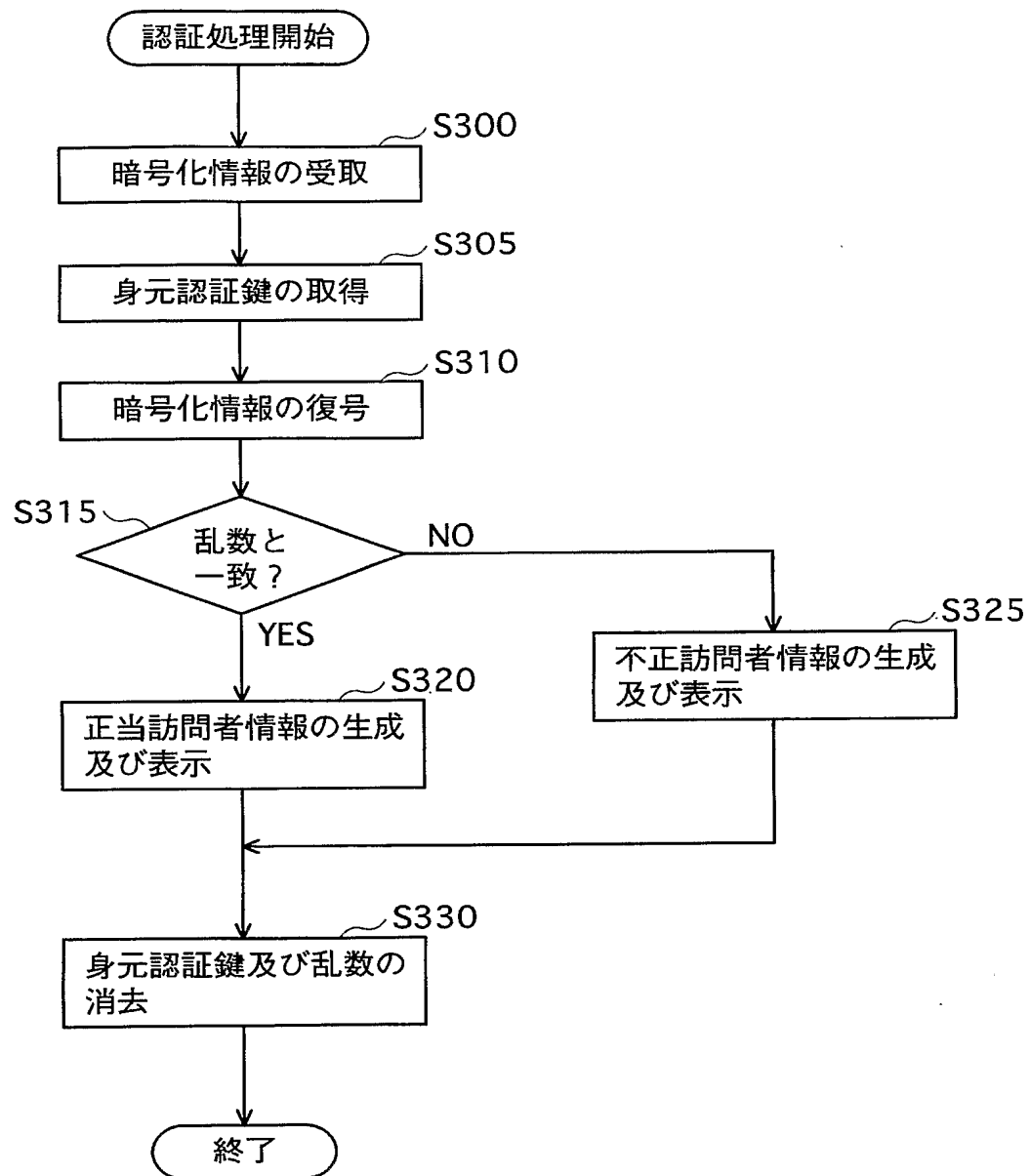
【図 12】



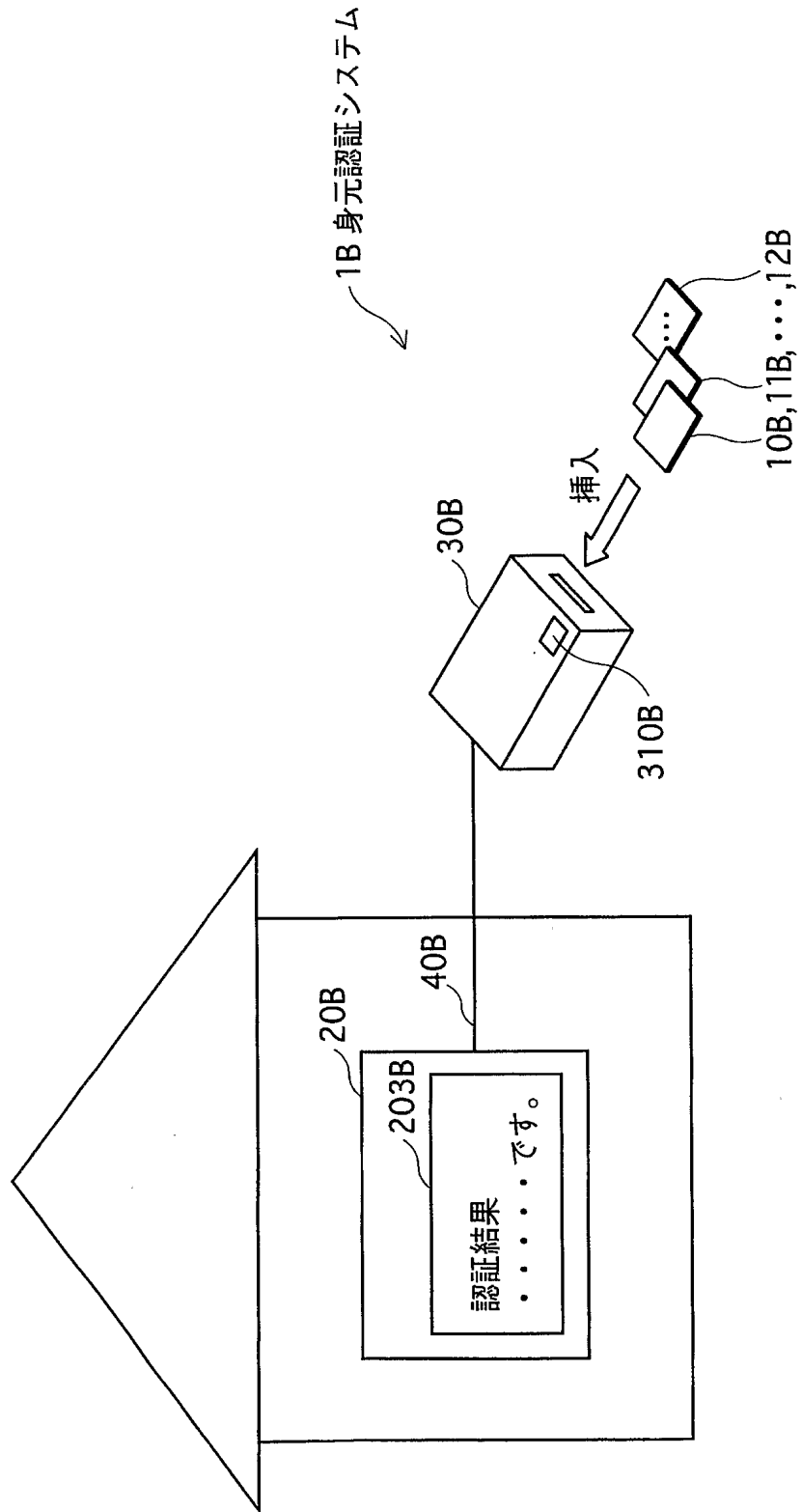
【図 13】



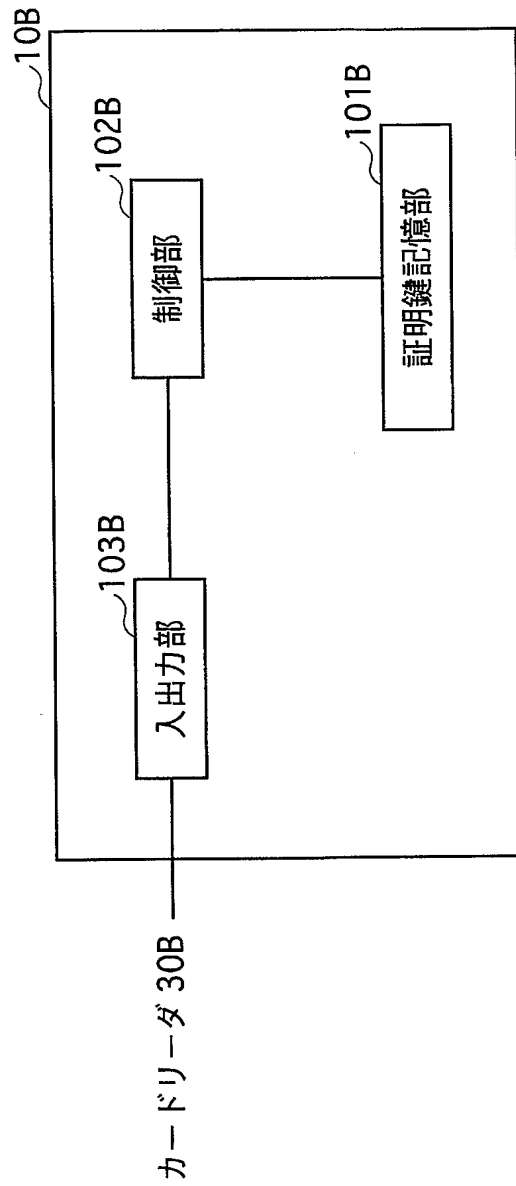
【図 14】



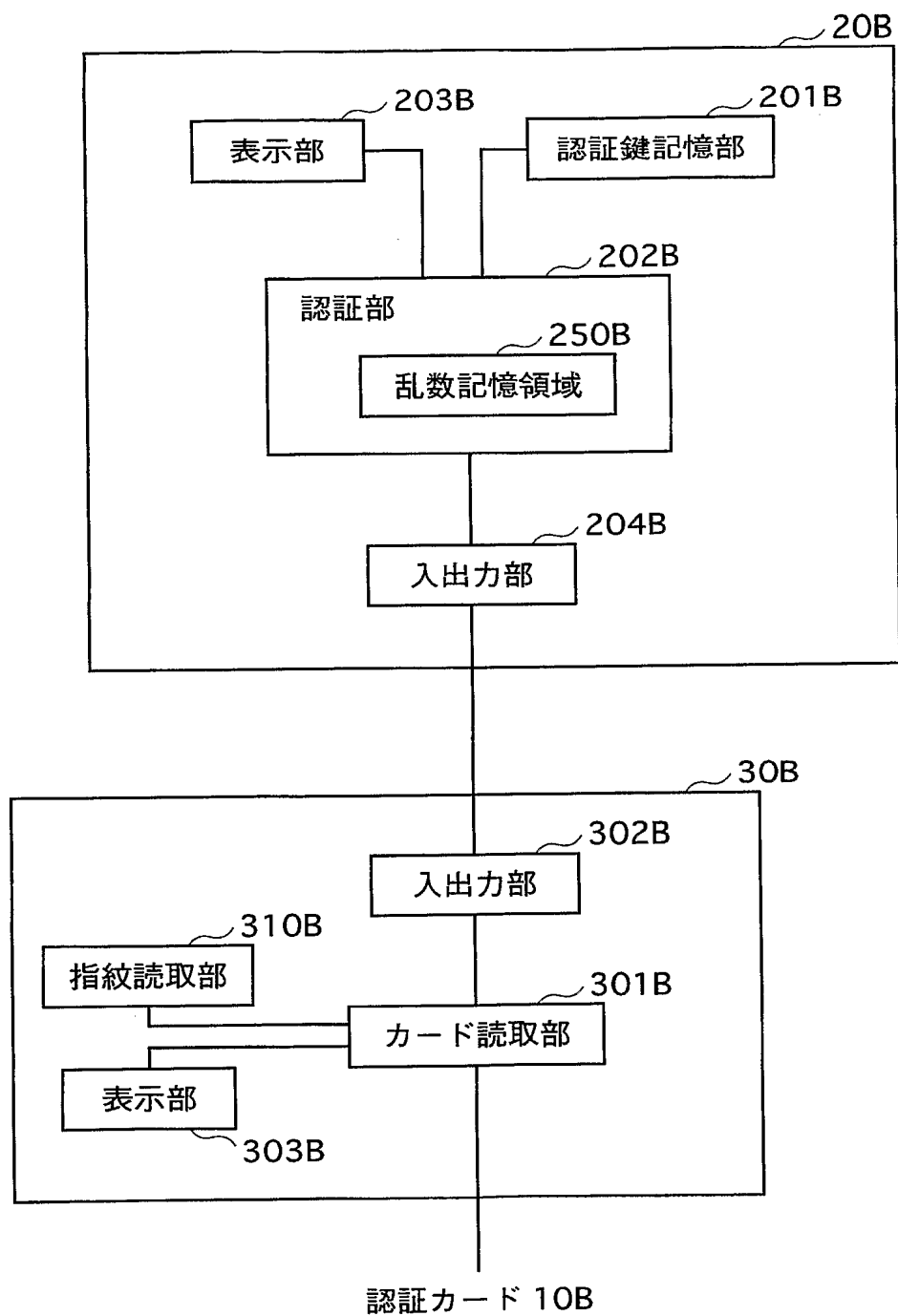
【図 15】



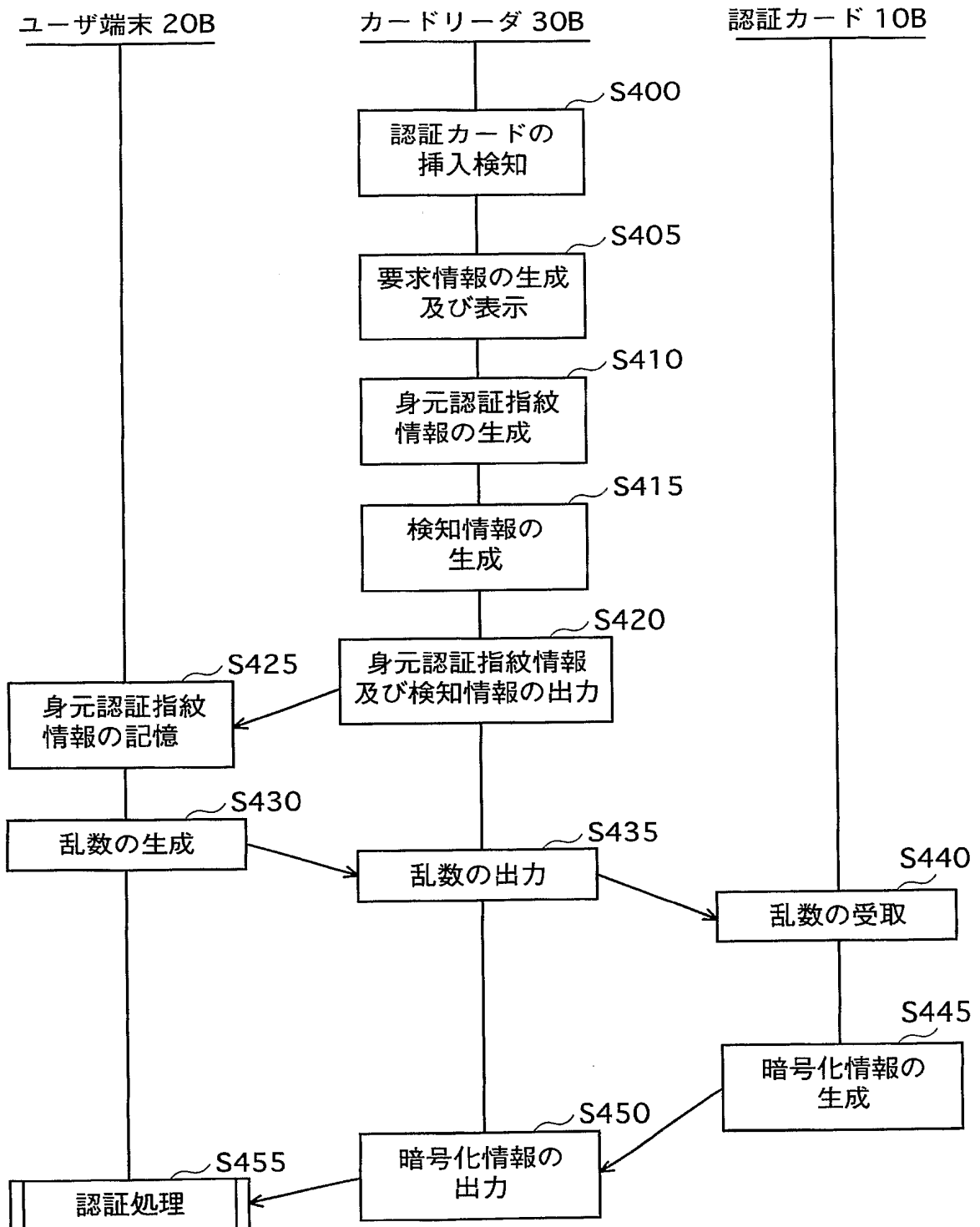
【図 16】



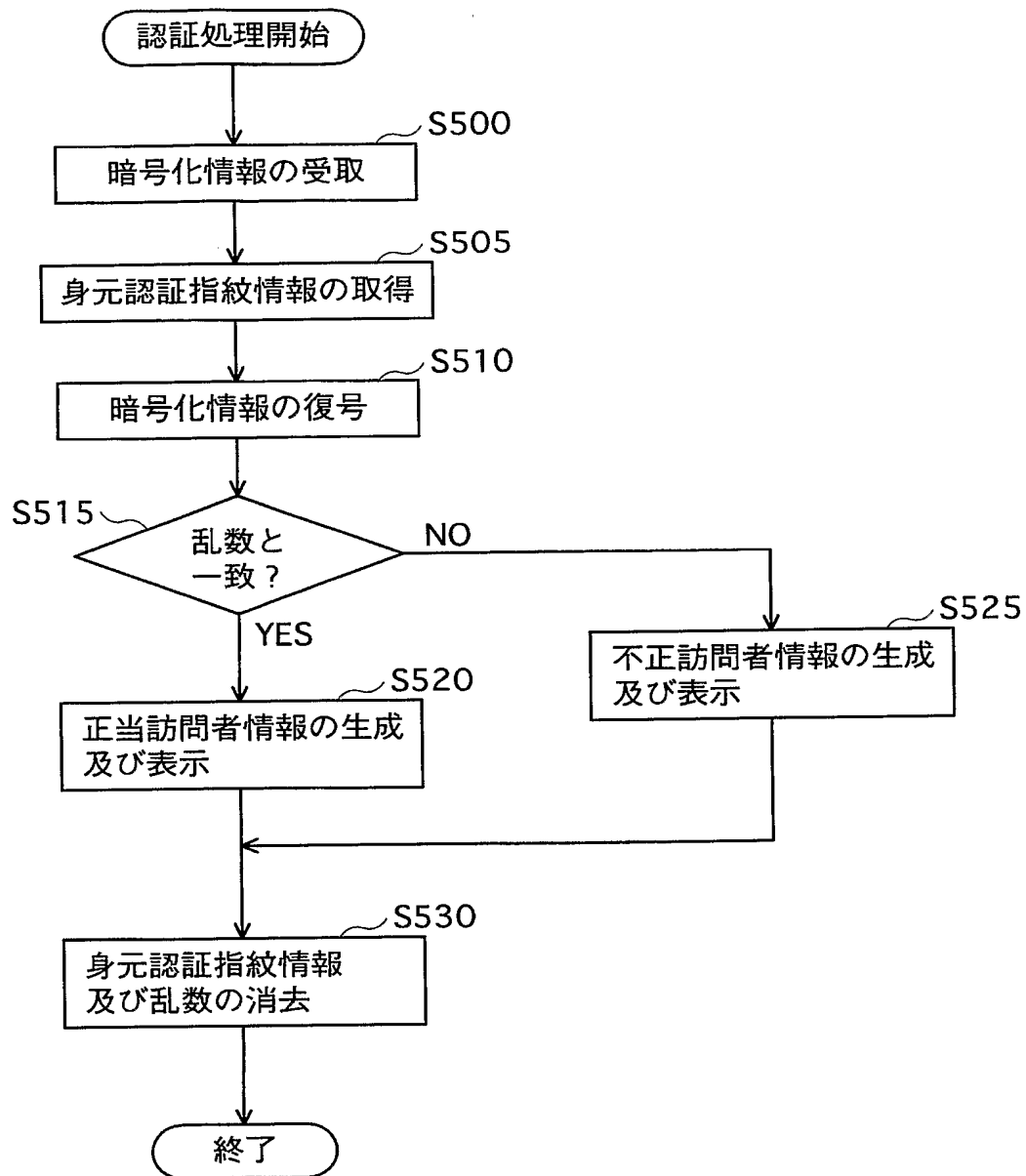
【図 17】



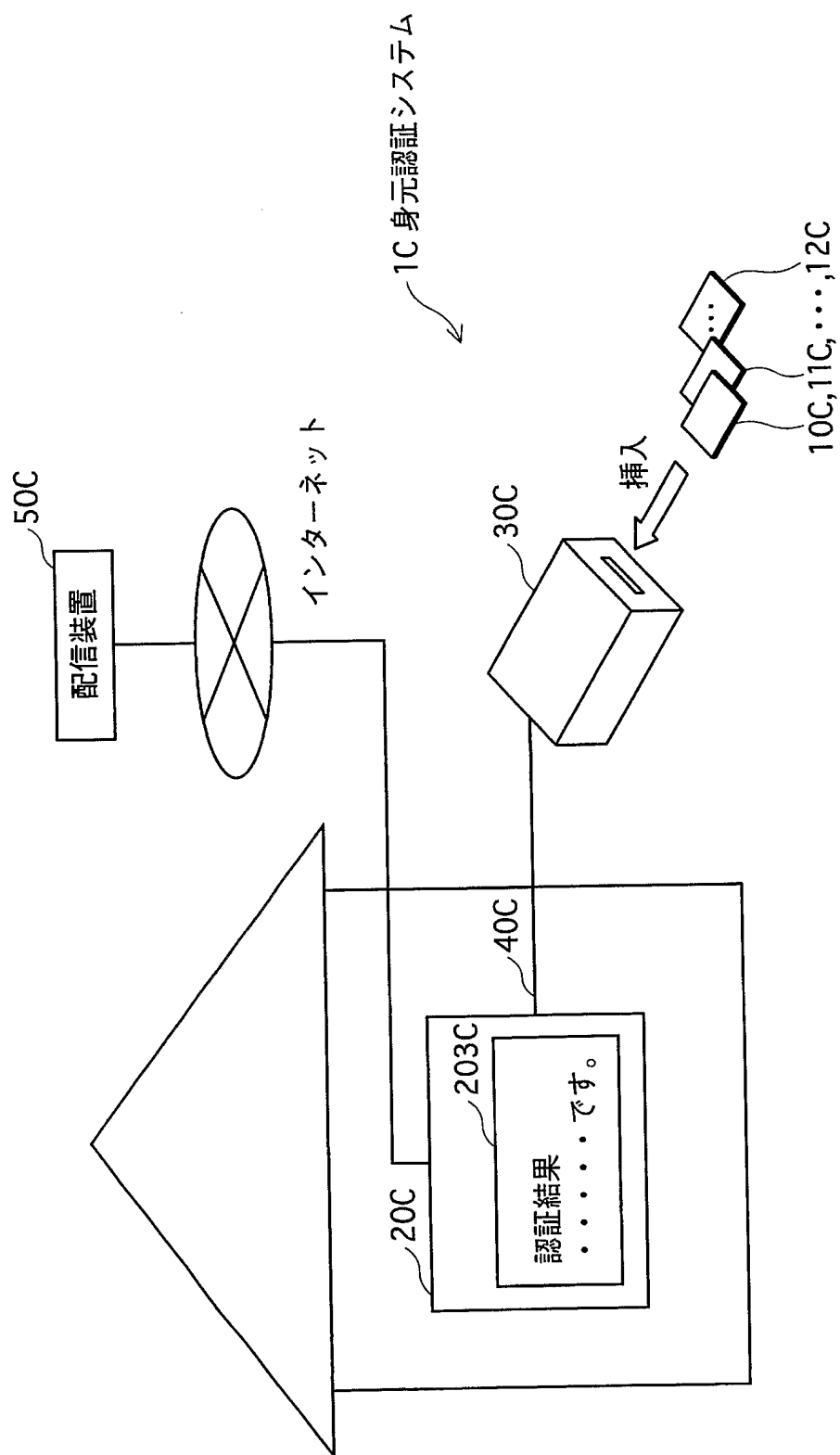
【図 18】



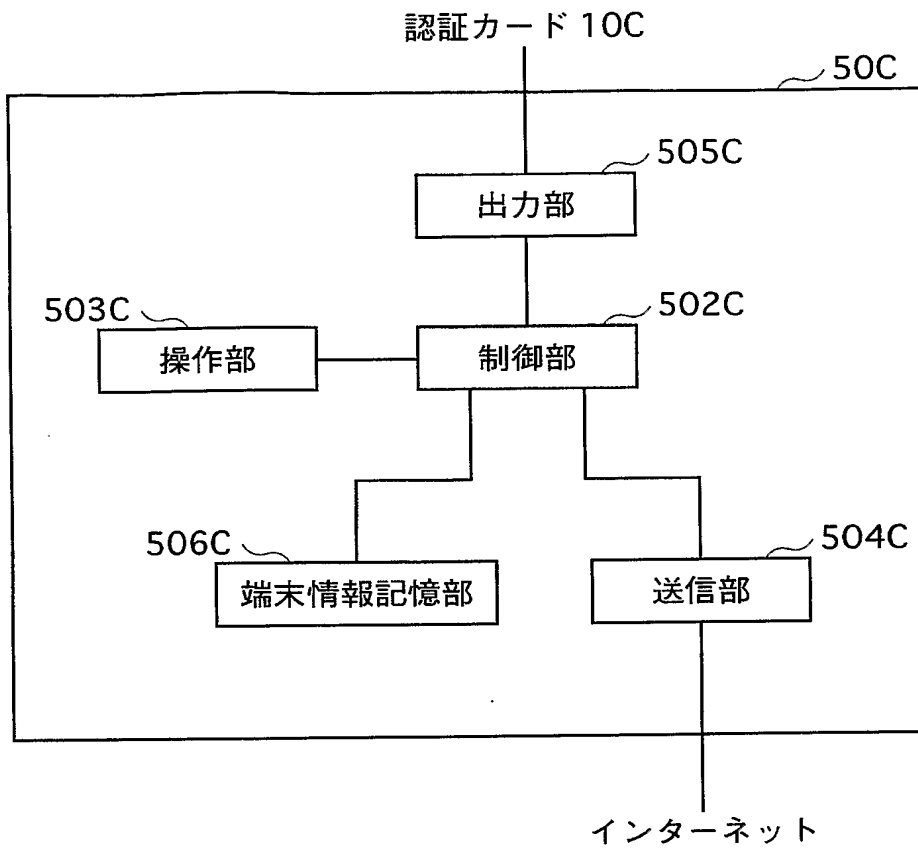
【図 19】



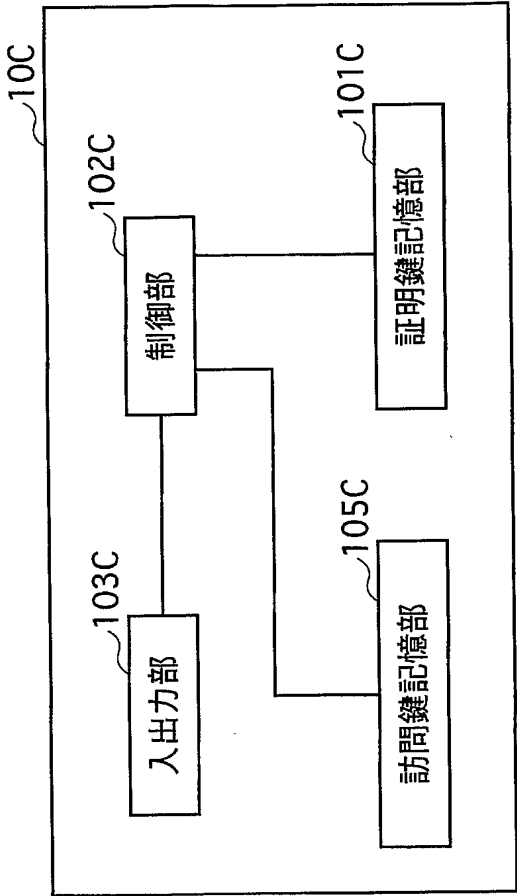
【図 20】



【図 21】



【図 2 2】

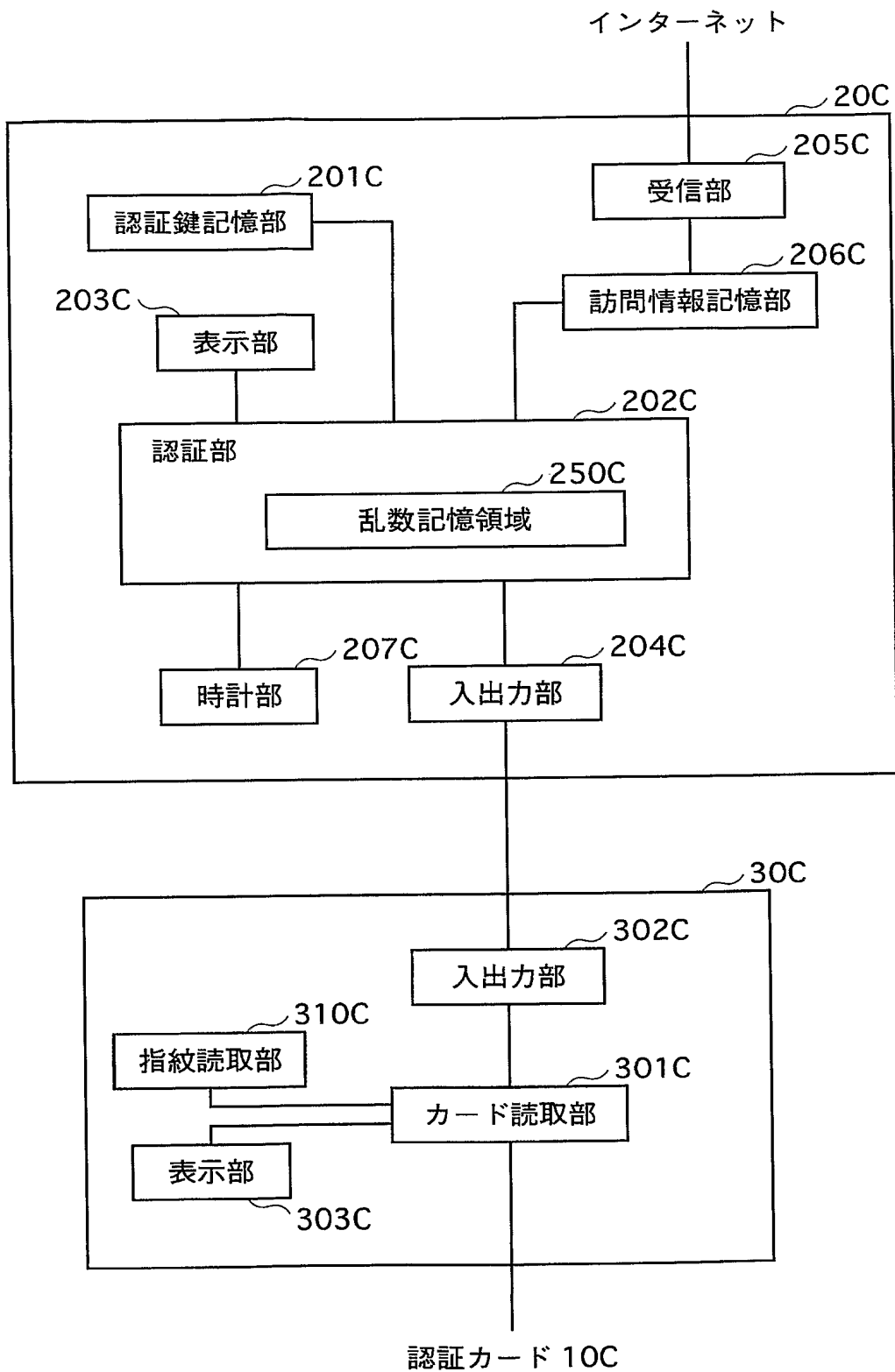


【図 2 3】

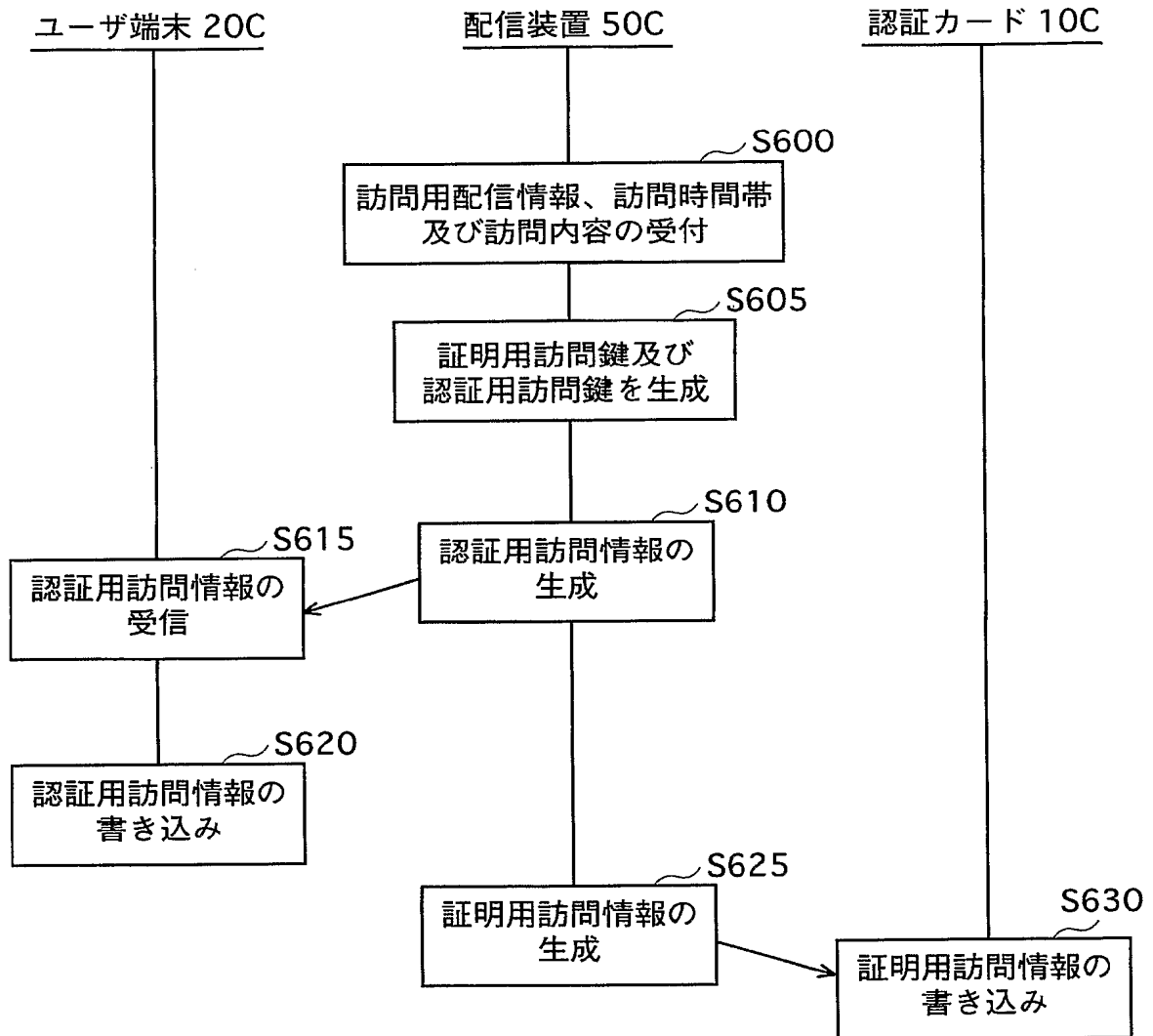
T300
↙

端末ID	訪問時間帯	訪問内容	訪問鍵
T-ID 1	13:00～15:00	物品A届	V-key1
T-ID 2	13:00～15:00	物品B届	V-key2
・	・	・	・
・	・	・	・
・	・	・	・

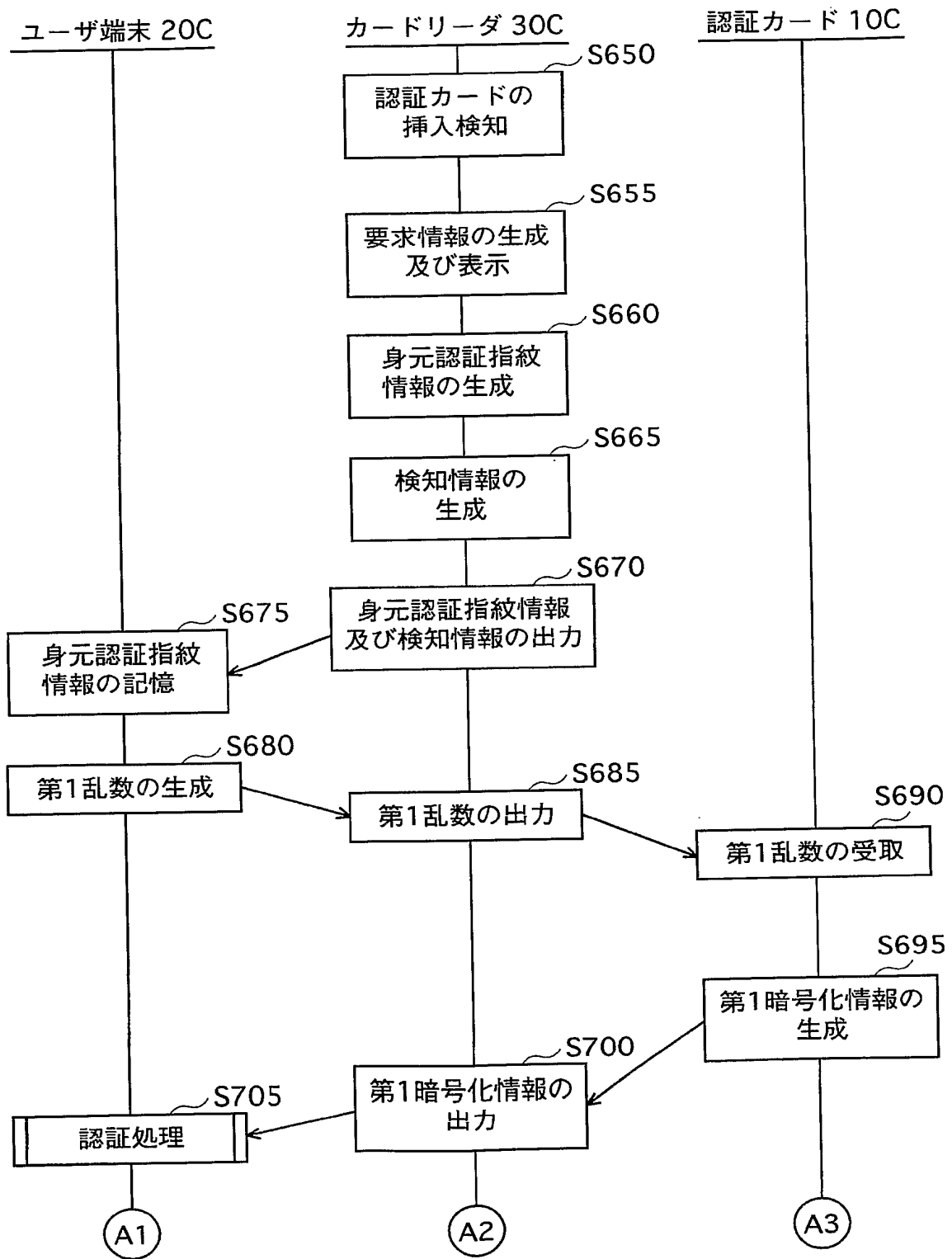
【図 24】



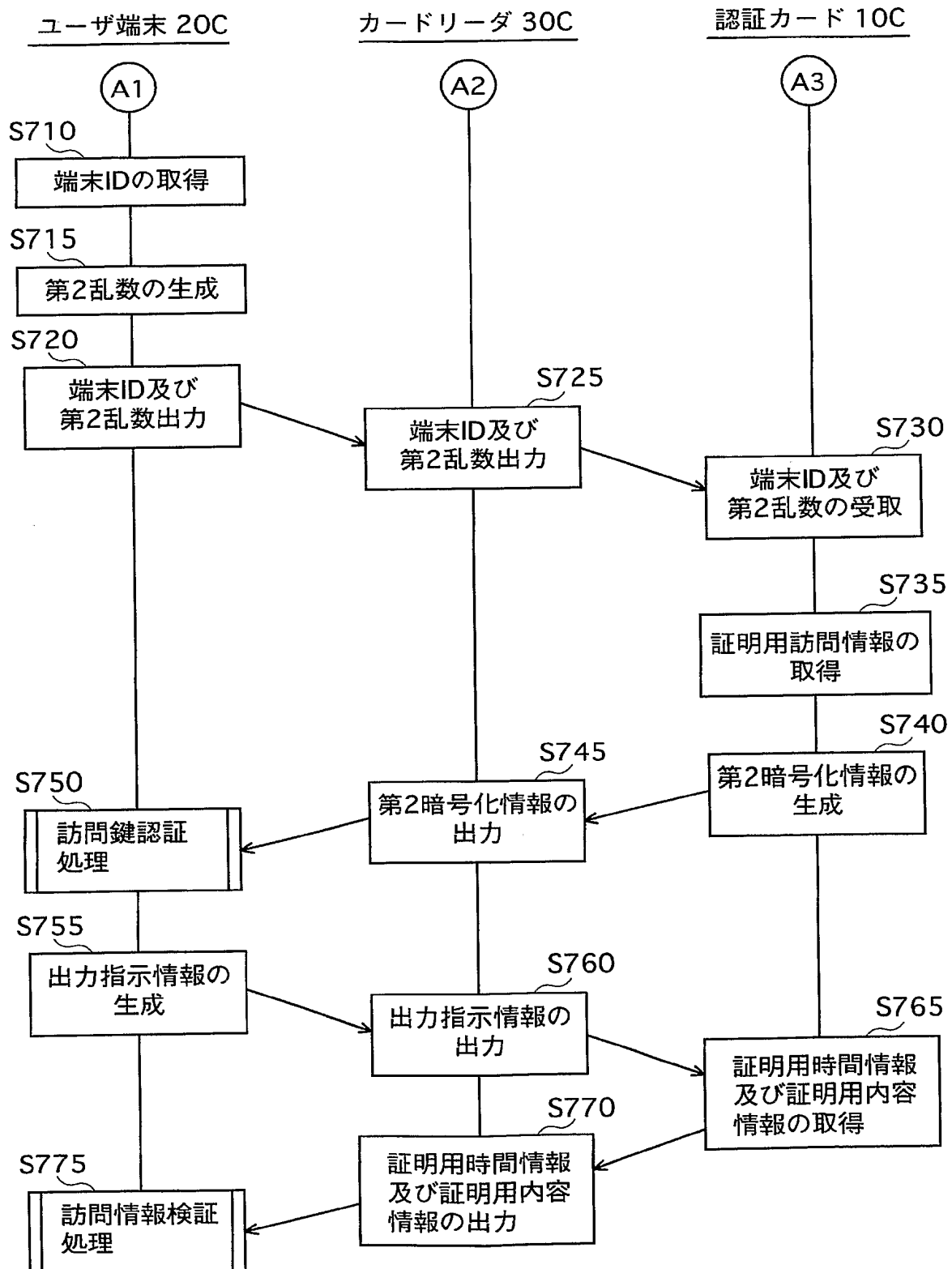
【図 25】



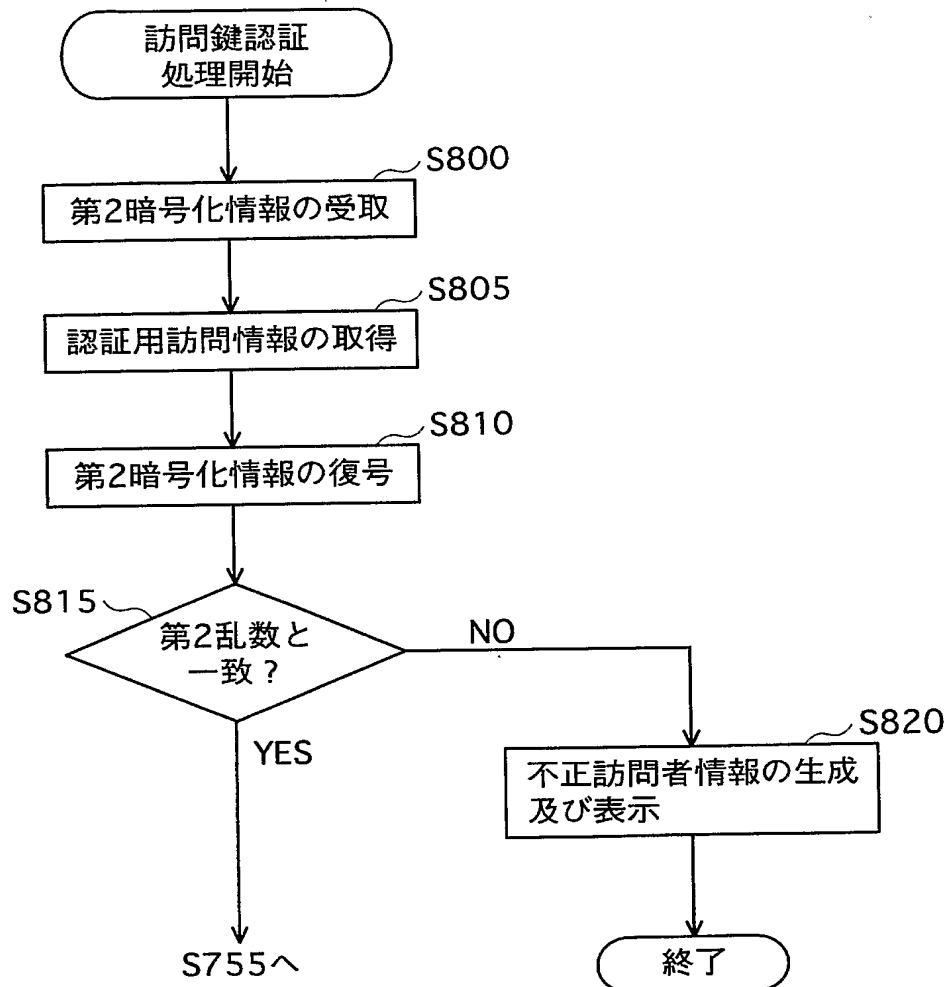
【図 26】



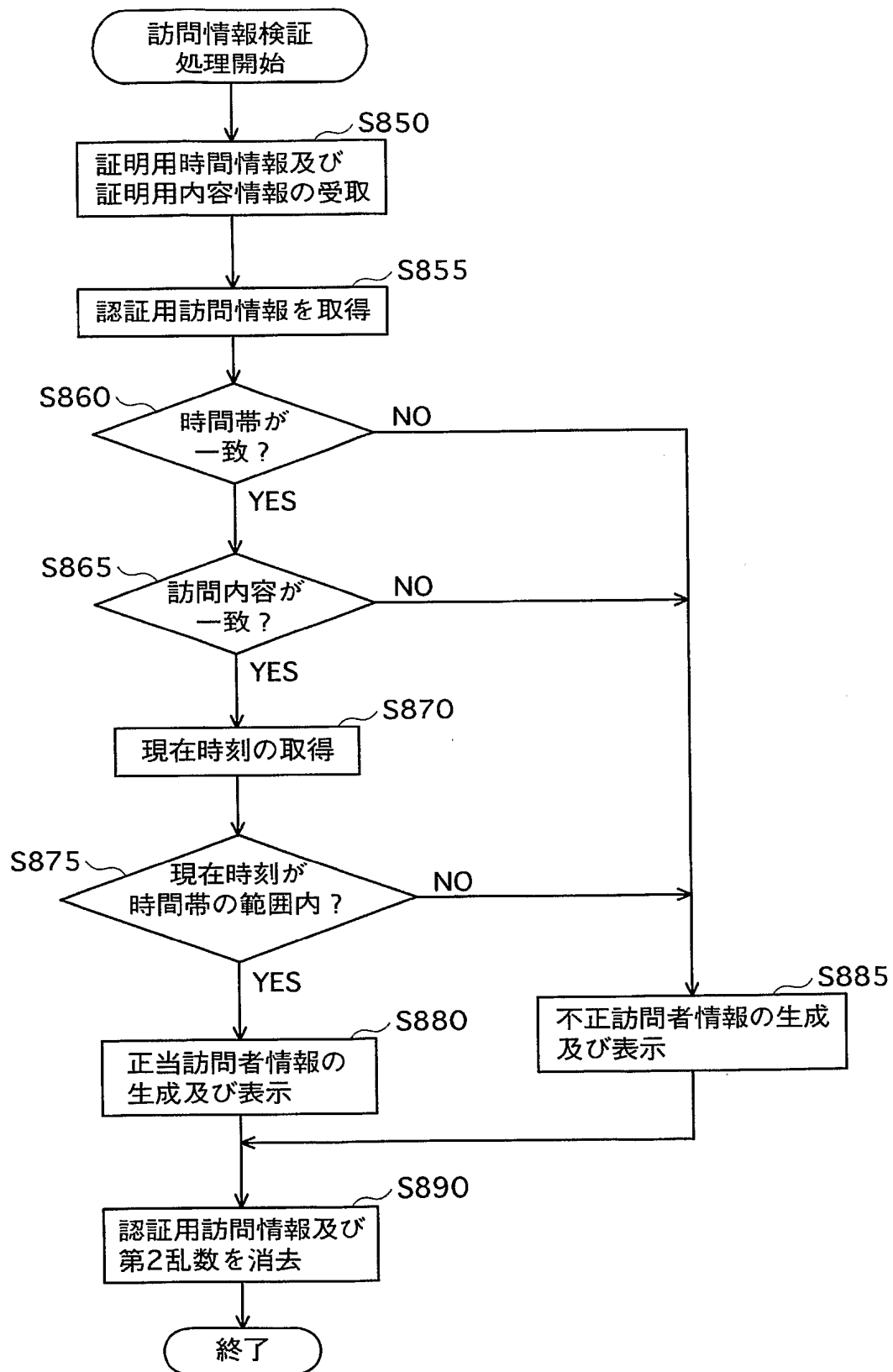
【図 27】



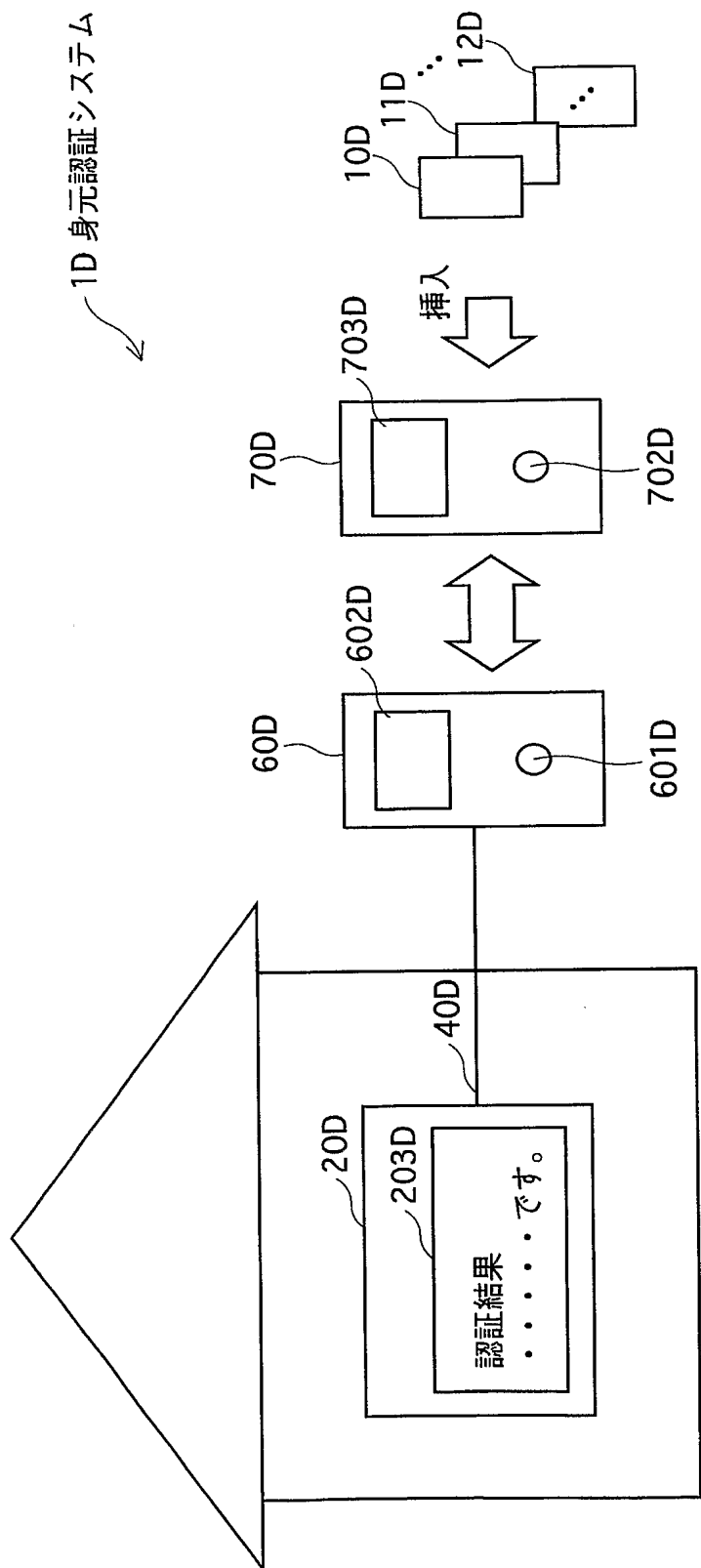
【図 28】



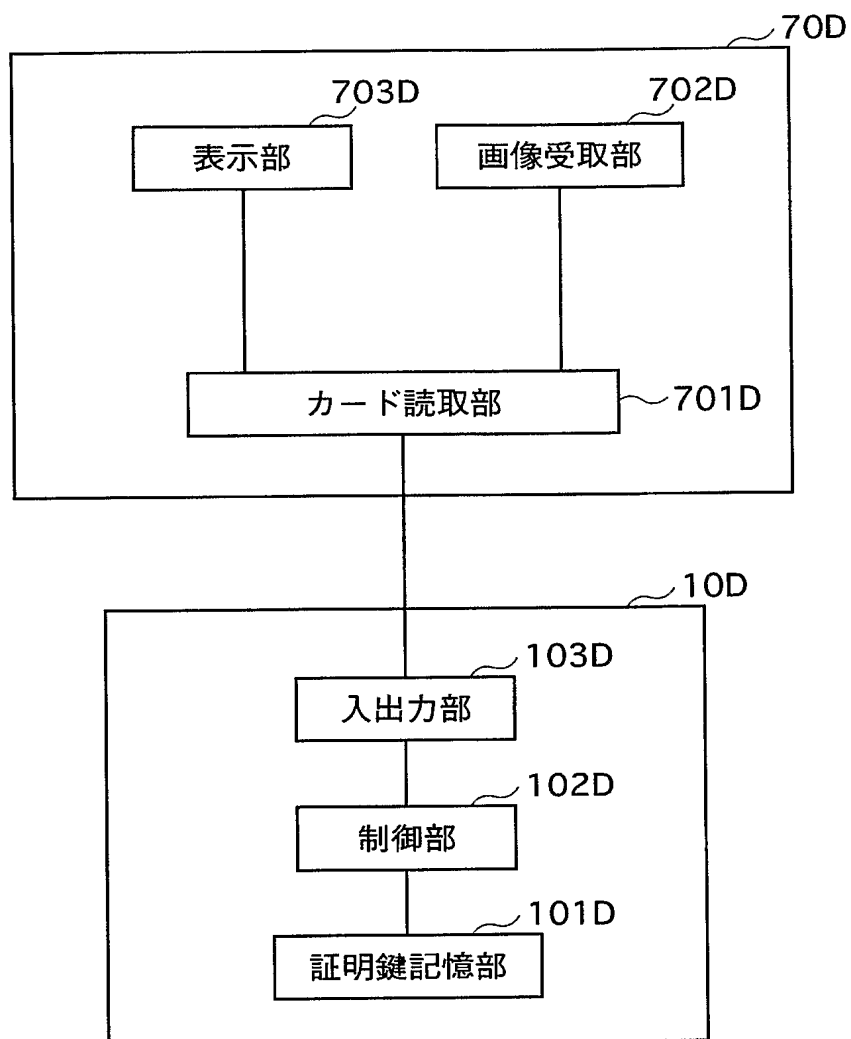
【図 29】



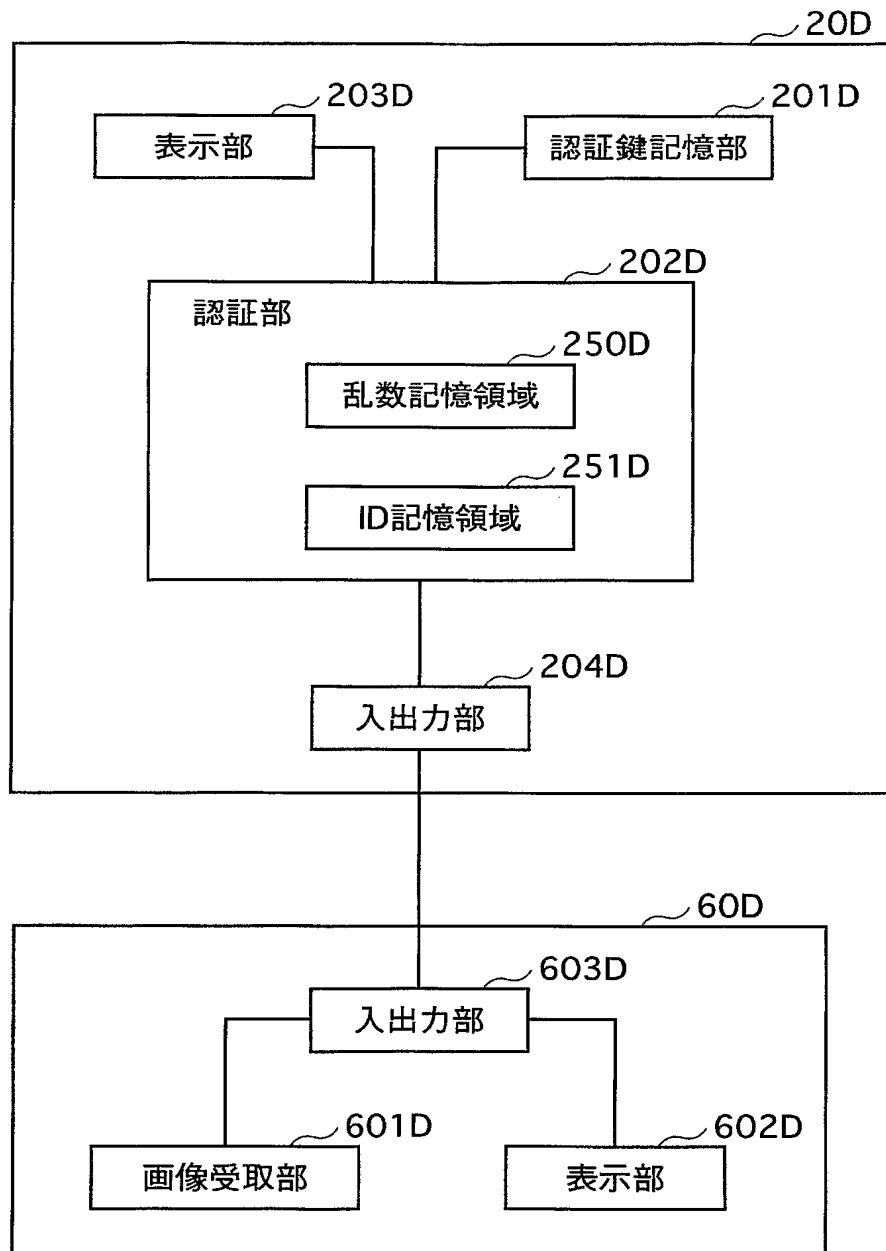
【図 30】



【図 31】



【図 3 2】



【書類名】 要約書**【要約】**

【課題】 常に訪問者の身元の認証を行うことのできる認証システムを提供する。

【解決手段】 身元認証システム 1 は、認証カード 1 0、1 1・・・、1 2 と、ユーザ端末 2 0 と、カードリーダー 3 0 とから構成される。

ユーザ端末 2 0 は、カードリーダー 3 0 に認証カード 1 0 が挿入されると、乱数を生成し、生成した乱数を記憶するとともに、認証カード 1 0 へ出力する。認証カード 1 0 は、予め記憶している身元証明鍵にて受け取った乱数を暗号化して、暗号化情報を生成し、生成した暗号化情報をユーザ端末 2 0 へ出力する。ユーザ端末 2 0 は、受け取った暗号化情報を予め記憶している身元認証鍵を用いて復号して、復号結果を生成し、生成した復号結果と生成した乱数とが一致するか否か判断することによる認証を行う。

【選択図】 図 1

特願 2 0 0 3 - 4 1 0 7 8 4

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 8 2 1]

1. 変更年月日 1 9 9 0 年 8 月 2 8 日

[変更理由] 新規登録

住 所 大阪府門真市大字門真 1 0 0 6 番地

氏 名 松下電器産業株式会社